TILBURG UNIVERSITY

Tilburg University

Design and analysis of covert networks, affiliations and projects

Lindelauf, R.

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
Lindelauf, R. (2011). *Design and analysis of covert networks, affiliations and projects*. [Doctoral Thesis, Tilburg University]. CentER, Center for Economic Research.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 05. May. 2023

Design and Analysis of Covert Networks, Affiliations and Projects

Design and Analysis of Covert Networks, Affiliations and Projects

Proefschrift

ter verkrijging van de graad van doctor aan Tilburg University op gezag van de rector magnificus, prof.dr.Ph. Eijlander, in het openbaar te verdedigen ten overstaan van een door het college voor promoties aangewezen commissie in de aula van de Universiteit op maandag 24 oktober 2011 om 14.15 uur door

Roy Hubert Albert Lindelauf

geboren op 6 december 1976 te Heerlen.

Promotores: prof. dr. P.E.M. Borm
prof. dr. H.J.M. Hamers

In loving memory of my father

Life is eternal;
and love is immortal;
and death is only a horizon;
and a horizon is nothing save the limit of our sight.

- Rossiter W. Raymond

'How vain it is to sit down to write
when you have not stood up to live.'
- Henry David Thoreau.

Acknowledgements

Thanks to Mum and Dad, who raised me in absolute freedom, and who instilled in me the belief that anything is possible as long as you are willing to fight for it.

Thanks to Yf, for being such a great listener and down to earth person. It is truly wonderful being your 'little brother', but above all, to be your friend. Thanks for booking the trips that took me all over this world.

Thanks to Jeannine. Life may lead us along different paths, but in the end we are both homeward bound. I know I can always count on you.

Thanks to Herbert and Peter. My impatience and haste must have been a continuous frustration for the both of you, and I am grateful for the (sometimes not so) gentle way you pushed me to my limits.

Thanks to Robbert, without whom I would never have considered going into academia and who gave me the confidence to create my own trail.

Thanks to the Heynen brothers - Rolf and Alexander -, Rene, Preveen and others. For helping me to relax at the right moments, and moreover, at the right places.

Thanks to the people at the AZM, AMC and Erasmus MC, but above all Ygal, whose skill and encouragement kept - and will keep - me going for years.

Thanks to those who were willing to read and comment on earlier versions of this manuscript. In particular I am thankful for the positive and encouraging criticism of the Ph.D. committee members.

Finally, thanks to the professional people in our Armed Forces, whose willingness to put their life on the line never ceases to amaze and inspire me.

Etten-Leur, August 2011
Roy Lindelauf

Contents

Chapter 1

Introduction

'Do not worry if you have built your castles in the air.
They are where they should be.
Now put the foundations under them.'
- Henry David Thoreau.

'A successful person is one who can lay a firm foundation with the bricks that others throw at him.'
- David Brinkley.

The study of covert phenomena in general and terrorism in particular is first and foremost a study in human behavior [Martin, 2006]. Research on terrorism and its phenomena is multidisciplinary in nature. Clearly, it is a fact that we are still very far from terrorism research being a unified science. It is therefore evident to give thought to the problem of the overall aims of this research domain. What are the essential questions that need answers, and why? What is terrorism? No single legally binding definition of this phenomenon has been established up to date. Political and emotional motives being the root cause of this status quo. For instance, in 1988 Schmid and Jongman counted 109 definitions of terrorism that covered 22 different elements [Schmid and Jongman, 1988]. There seems to be even much less agreement about the definition of covert phenomena in general.

In decision making aimed at confronting covert organizations managers are faced with high-level, long-term planning issues characterized by an uncertain and complex networked environment. The amalgam of opponents in Afghanistan that confront ISAF and Operation Enduring Freedom for instance should be viewed as interdependent rather than independent, autonomous units. These opponents exchange information via communication networks, diffuse weapons through trafficking networks and their Shura councils

meet in affiliation networks. Understanding the effects of such a complex operational environment and evaluating its social aspects becomes extremely important in launching a successful counterinsurgency campaign, a fact recognized by the U.S. counterinsurgency doctrine [Petraeus et al., 2007].

Closer at home the threat of terrorism changed face after the tragic events of 9/11, Madrid and London. Much of the research and policy interest to the problem of terrorism that followed those events consists of efforts to identify the terrorists using large amounts of data. Law enforcement agencies have been dealing with related problems for decades. They are interested in how to identify those members of a criminal organization that are important or require more attention than others, to figure out their role in the organization (if any) and how to disrupt criminal operations. Traditionally such questions were (and still are) answered by meticulous field investigations and qualitative analysis of reports and other sources of data. Additionally social network analysis (SNA) has become a prevalent tool in this endeavor. This tool is a mix of sociology and techniques from mathematical modeling, especially graph theory. SNA is an example of how mathematical modeling can aid in the analysis of terrorist and criminal organizations. However, as mathematics consists of hundreds of specialized areas, there are numerous other ways in which mathematical modeling can contribute to the study of covert phenomena. Motivated by the existence of large volumes of data but few exact models of covert organizations, the presence of sophisticated modeling techniques in different domains, and the desire to understand covert phenomena, this thesis sets out to develop and analyze models of covert organizations. In the following sections we will present some more background information and the layout of this thesis.

1.1 Modeling covert organizations

How should we study covert organizations and the myriad of forms in which they appear? And above all, what method if any suffices to study them? Perhaps one should start by accepting that covert phenomena are too complex to study in their entirety. Instead, if impossible to study in their entirety, we should reduce it into as many parts as necessary and study them individually.

First there is a need for descriptive work. The collection of observations, such as the interrelationships between individuals engaged in terrorist attacks for instance, should always be a basic part of this science. The problem with accurate observations is that they mostly exist within the realm of intelligence, unaccessible by scholars not related to

the intelligence community. Clearly the historian and political scientist play a prominent role in this endeavor. However due to the increasing amount of 'digitization' of our society the ability to map and store human behavior during terror related events becomes increasingly possible. Therefore the computer scientist also figures prominently among the 'collectors'.

Second, these descriptions of observable phenomena should lead to theories that help understand these phenomena and make predictions that can be refuted by observations. Such theoretical reasoning can both be from a qualitative or quantitative viewpoint and therefore mathematicians, computer scientists, sociologists, psychologists, organizational scientists, anthropologists and other scholars all participate in this endeavor. The observable covert phenomena that are dealt with in this thesis include the networked organizational form of covert organizations, the ability of such networks to withstand disruption and the identification of key leaders in such organizations based on the structural position they hold with respect to the social network or the tasks they enable in terror plots. The methodology we use is quantitative, more specifically we develop and use game theoretical and graph theoretical modeling. So what are the myriad of forms in which covert phenomena occur and in which they can be studied?

First consider the networked organizational form of covert organizations. As the Mumbai attack of 26 November showed, modern technology acts as an enabler and force multiplier for terrorists. Tactical commanders and individual team members used satellite and cell phones to connect to the strategic commanders outside of the area of operations. Multiple teams consisting of several individuals each were able to communicate and direct each other as the attacks progressed. What set apart those attacks, however, is not the use of technology per se; it is the networked mode of operation that is enabled by technology. The organizational form among these attackers is not easily characterized as being hierarchical or decentralized, but the underlying mechanism to all these operations is the networked topology.

Different perspectives exists on the organizational structure of groups engaged in the worldwide religious revivalist movement [Mishal and Rosenthal, 2005]. For instance: is Al-Qaeda a corporation, a franchise organization, or an ideological movement? In answering this question, most analysts nowadays would tick the all-of-the-above box. Al-Qaedas core leadership, mainly operating from the Pakistani Northwest Frontier Province region, is reduced in size and only performs a peripheral function with regard to day-to-day operations. However, its franchise movements ranging from Indonesia, the Maghreb and Europe are active in the formation of underground cells [Vidino, 2007]. Researchers argue

that the basic covert organizational forms most commonly observed in such networked organizations are the chain network in smuggling operations, the star network found in cartels, and the all-to-all network in militant peace groups [Arquilla and Ronfeldt, 2001]. Clearly, hybrid networks that are a mix of these basic networks can and will also be found in covert networked organizations. The question becomes what network topologies covert organizations such as Al-Qaeda or Hezbollahs underground wing adopt and why. This question can be analyzed by considering the critical dilemma such organizations have to solve: how to efficiently coordinate and control while at the same time remaining secret. Answers to this question from the perspective of *simple* covert networks, using graph theory and game theoretic bargaining, will be formulated in chapters 3 and 4. In chapter 5 we discuss covert organizational design issues of *affiliation* networks.

Next consider the concept of resilience, i.e., 'an organization's ability to survive, and potentially even thrive, in times of crisis' [Seville et al., 2006]. It is known that some covert organizations are more resilient than others. It can be argued that this resilience among others depends on the network structure of the covert organization. In chapters 3 to 5, which are based on Lindelauf et al. [2009a,b, 2010], it is argued that secrecy is an important design parameter in setting up this network structure of a covert organization. In general one can argue that, even if covert organizations do not explicitly take secrecy into account, they adopt network structure designs that develop implicitly due to trial and error. Therefore one might wonder about the effect of disruption activities on the functioning of the covert network.

This resilience aspect of networks has been studied abundantly by scientists outside of the covert network domain. For instance: if we have information or disease propagating through a network, how robust is this propagation to failure or removal of vertices? The relevance of this question to a counterinsurgency campaign is clear: one wants to affect the social structure in such a way to provide sustained security for the population. In other words: one wants to make sure that the different paths by which insurgents spread fear among the population are being reduced as much as possible by carefully selecting and isolating nodes in the network, similar to the reduction of epidemics by immunization against the spreading of a disease [Ball, 1997].

Resilience studies of covert organizations in the qualitative literature are based on theories of charismatic leadership or basic social network analysis. In chapter 6, which is based on Lindelauf et al. [2011], we analyze this problem from a quantitative viewpoint by studying the effect of the removal of members of a covert organization on the optimality of its network design for which we laid the groundwork in chapters 3,4 and 5.

Another approach to the study of covert organizations is the identification of key leaders. It is claimed in the 2003 National Strategy for Combating Terrorism that leaders are essential to terrorist activity and that their removal is likely to result in organizational collapse [Jordan, 2009]. In chapter 7 we will therefore focus on the identification and characterization of key leaders in covert *networks* and in chapter 8 we focus on key leadership with respect to covert *projects*.

Traditionally social network analysis focuses on questions of centrality: who are the key players in the network? A plethora of measures have been developed to answer this question; both from a mathematical as well as from a sociological viewpoint. The application of such centrality measures in particular, and network theory in general, is only useful if the practitioner and the theorist are on an equal footing. The methodologist has to ground his theory in observable facts based on an intimate knowledge of the social environment he is modeling. He can come by this knowledge only when working closely with those having their boots on the ground. Vice versa, the practitioner can hugely benefit from insights obtained by methodologically analyzing carefully constructed databases that reflect the social complexity at hand. It can help him to more efficiently and effectively find and eliminate the enemy groups in his area of operations.

Most quantitative analysis of covert networks up to date rely heavily on methods developed in (applied) graph theory [Lindelauf, 2009]. One of the most intriguing questions in network analysis is how to quantify the intuitive feeling that in most networks some of the players are more important than the others. To this aim many centrality measures were introduced, starting for the first time in the 1950s [Bavelas, 1948, 1950]. Since there are so many different centrality measures one can wonder what the added value of game theoretic modeling in determining the power of players in networks is. The usefulness of game theoretic modeling becomes clear when we consider the nature of the data available on covert networks as we will illustrate in chapter 7. Data on terrorist phenomena consists of a lot more than just network data. In general such data consists of all kinds of human behavior patterns, i.e., the data captures interactions between individuals as well as data on the individuals themselves. Consider for instance telecommunication data consisting of location data (so-called player-related information). Additionally it can be said that generally the interaction between individuals is heterogeneous, i.e., those interactions can be of all sorts and types. Consider the exchange of information by telephone or data that reflects family relationships (we call these kind of data *relationship*-related information). The most often employed standard centrality measures degree, betweenness and closeness only take the network *structure* into account and ignore other variables and parameters that in practice are often available. This fact is acknowledged by Newman [2004]:

"Recent studies of networks have, by and large, steered clear of such weighted networks, which are often perceived as being harder to analyze than their unweighted counterparts."

The networks carrying additional information that Newman studies are of a very specific type, because in those networks the relationships between individuals are weighted. Standard centrality measures that incorporate such additional information can only assign unique values to at most *pairs* of individuals. However, in chapter 7 we will show that game theory allows for a much more generalized analysis of centrality of players by allowing the assignment of unique values to *each* possible coalition of players.

Cooperative game theory assigns values to the coalitions of players, using the so-called characteristic function. On the basis of one-point solution concepts for cooperative games, rankings of players can be created. One of the most common one-point solution concepts for cooperative games is the *Shapley value* [Shapley, 1953]. Intuitively it computes a weighted average of the marginal contribution of a player to coalitions. An explicit definition and discussion of this power index will be given in chapter 7. When we assign a value to a coalition, we in fact are considering the context under consideration. In the case of modeling covert networks one has to take all available information concerning the situation at hand into account. Another game theoretic solution concept, the compromise value, will be discussed and used in chapter 8 to illustrate the identification of key players in a covert project.

1.2 Contribution

The contributions of this thesis can be divided into four topics. These topics include the design of covert networks, the design of covert affiliations, the analysis of covert networks and the analysis of covert projects.

The first topic, the design of covert networks, is inspired by the fact that many analysis of covert networks are of a qualitative nature. In this thesis formulas are derived that quantify the essential considerations a covert organization faces. The resulting framework on covert network design is presented and several approximations are given in case of large covert networks [Lindelauf et al., 2009a]. The covert network model is analyzed from several different perspectives and multiple scenarios are presented. Such scenarios can be used as training and test sets for reasoning about covert networks. A different approach to covert organizational design is by viewing covert organizations from the perspective of affiliations. We present covert affiliation designs, analyze the performance of three basic covert affiliation networks, and present a procedure that optimizes hypertrees with respect

to secrecy and information performance. Moreover we show that in certain cases star-like structures are optimal [Lindelauf et al., 2010]. The third topic of this thesis, the analysis of covert networks, is an extension of work on overt networks to the covert network domain and essentially consists of two parts. The first part considers the structure of the network as a whole and in the second part the analysis focuses on finding 'important' individuals within covert networks. Concerning covert networks as a whole it is shown on both theoretical as well as empirical grounds that covert networks are not 'small-worlds' [Lindelauf et al., 2011]. Additionally resilience studies show that disruption strategies focused on capturing or isolating highly connected individuals are not that effective. The second part on covert network analysis focuses on finding individuals that are important in some sense in the covert network. Finding such individuals from a large set of data is important since in practice intelligence and law enforcement agencies have limited resources at their disposal which means that only a limited number of individuals can be investigated. Traditionally social network analysis is used as a quantitative tool to aid in the analysis of such data-sets. However this methodology often neglects additional information that is available. Our contribution to the area of finding key players is first by introducing an approach to model the additional information that is present based on cooperative game theory. Second we present and analyze a method to identify the key players if the data consists of the tasks that individuals enable in a covert project.

1.3 Outline

In chapter 3 we will introduce a mathematical model that is used to explain and investigate the structure of covert networks based on Lindelauf et al. [2009a]. This is done by defining an information measure, secrecy measure and a measure capturing the tradeoff between information and secrecy (Section 3.3). Next we analyze the model by considering three specific scenarios in Section 3.4. To investigate the robustness of the results a variation on the information is introduced in Section 3.5 and optimal networks are analyzed and compared with the initial findings and optimal covert network structures are presented for larger order graphs.

In chapter 4, based on Lindelauf et al. [2008, 2009b], the basic (homogeneous) covert network model as introduced in chapter 3 is extended by introducing heterogeneity with respect to secrecy and information. We introduce two empirical examples in Section 4.2 to motivate an extension of the secrecy measure by introducing weights on the links representing the risk of interaction. In Section 4.3 it is shown that the pair of individuals in the organization that should conduct the interaction that presents the highest risk to

the organization is the pair that is the least connected to the remainder of the network. In Section 4.4 we will discuss secrecy *and* information heterogeneity and analyze a star network example.

In chapter 5 we focus on the participation of covert individuals in events (or cells), instead of looking at a covert organization from the perspective of relationships between individuals. Chapter 5 is based on Lindelauf et al. [2010]. In the sociological domain such structures are termed affiliation networks. Again we examine the secrecy versus information tradeoff dilemma a covert organization faces, but now from the perspective of affiliation networks. In Section 5.2 we present an example of such a covert affiliation network and we formally define several standard affiliation networks representing basic covert network organizational designs. In Section 5.3 we analyze covert affiliation network performance and in Section 5.4 we will show that 'star-like' affiliation networks are optimal in the secrecy versus information tradeoff. Section 5.5 finally discusses heterogeneous affiliation network topologies.

The design of covert networks and affiliations was the main topic of chapters 3 to 5. Upon the assumption that real covert organizations actually adopt such topologies one might wonder how good these structures actually are against disruption and removal of its elements. A field within network science has studied such problems in case of overt networks under the header of 'network resilience'. In chapter 6, based upon Lindelauf et al. [2011], we use and extend these ideas to investigate resilience properties of covert networks. First we investigate in Section 6.3 whether covert networks can be typified as small-worlds. Next to presenting some examples we discuss resilience in Section 6.5 and find the counterintuitive results that optimal covert networks might be well equipped to withstand targeted removal strategies.

In chapter 7 we shift the focus of our investigation towards the analysis and determination of the most important players in covert networks. We analyze standard centrality measures that find common usage in practice and also introduce game theoretic centrality measures that are better equipped to provide tailor made solutions. In Section 7.2 we introduce these measures and in Sections 7.3 and 7.4 respectively we apply these measures to two real-life case studies, being Jemaah Islamiyah's Bali attack and Al Qaeda's 9/11 attack.

In chapter 8 we analyze covert organizations by considering the underlying structure of the relation between players and tasks in projects such organizations conduct. Such projects for instance can be IED attacks, the production and distribution of synthetic drugs or nuclear proliferation. Data obtained by law enforcement and intelligence agen-

cies may also contain information of the nature of individuals engaged in one or more of the tasks that make up such a project. Hence if quantitative methods exists (or can be formulated) that can help analyze these kind of data and produce rankings of players engaged in such projects, that would contribute to the understanding of such organizations. In chapter 8 we present exactly such a method. After presenting preliminaries and notation (Section 8.1 and 8.2) we will introduce a project power measure that partitions the set of players that enable covert projects in three groups: core leaders, peripheral leaders and inessential players. In addition we characterize this power measure by use of several axioms. In Section 8.4 we introduce a class of corresponding cooperative games, so-called project games, and we will show that the compromise value of these games equals the project power measure. In addition we analyze the structure of the core of project games and relate it to the critical task group vectors.

Chapter 2

Mathematical background

In this chapter we present basic definitions and notions as will be used throughout this thesis. The words *graph* and *network* will be used interchangeably throughout the text as well as the words *hypergraph* and *affiliation network*.[1]

For a finite set N, we denote its power set, i.e., the collection of all its subsets by 2^N and its number of elements by $|N|$. For a finite set N and a subset $S \subset N$, we denote by e^S the vector in $\mathbb{R}^N$ defined by $e_i^S = 1$ for all $i \in S$ and $e_i^S = 0$ for all $i \in N \setminus S$. An *ordering* of the elements in N is a bijection $\sigma : \{1, ..., |N|\}$, where $\sigma(i)$ denotes the element in N that is at position i. The set of all $|N|!$ orderings of N is denoted by $\Pi(N)$.

A graph g is an ordered pair (N, E), where N represents the finite set of players[2] and the set of edges E is a subset of the set of all unordered pairs of players. An edge $\{i, j\}$ connects the vertices i and j and is also denoted by ij. For $V \subset N$, the V-induced subgraph of g is the graph $g' = (V, E')$ whose edge set E' consists of all the edges $ij \in E$ of the original graph g that connect players $i, j \in V$. The order of a graph is the number of vertices $|N|$ and the size equals its number of edges $|E|$. The set of all graphs of order n and size m is denoted with $\mathbb{G}(n, m)$. The set of graphs of order n is denoted by $\mathbb{G}^n$.

The degree of a vertex is the number of vertices to which it is connected. We denote the degree of vertex i in graph g by $d_i(g)$. The star graph on n vertices is denoted by g^n_{star}. We denote a ring graph of order n with g^n_{ring} and a path graph of order n with g^n_{path}. A complete graph of order n is denoted with g^n_{comp}. See an example of standard graphs of order 5 in Figure 2.1 below.

[1] For a general overview of graph theory we refer to Bollobas [1998], Bollobas [1986].

[2] A player is modeled as a node in a graph and represents an individual terrorist, insurgent or criminal engaged in a covert organization.

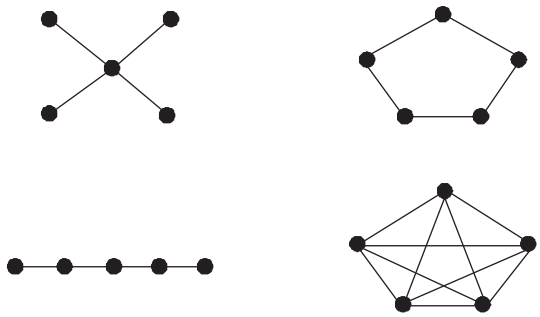


Figure 2.1: Star graph of order 5 (top left), ring graph of order 5 (top right), path graph of order 5 (down left) and complete graph of order 5 (down right).

The shortest distance between vertices i, j in g is denoted by $l_{ij}(g)$. Clearly, $l_{ij}(g) = l_{ji}(g)$. We will write l_{ij} instead of $l_{ij}(g)$ if there can be no confusion about the graph under consideration.

The total distance $T(g)$ in the graph $g = (N, E)$ is defined by $\sum_{i,j} l_{ij}(g) = \sum_{i \in N} \sum_{j \in N} l_{ij}(g)$. The diameter $D(g)$ of a graph $g = (N, E)$ is defined to be the maximum over the shortest distances between all pairs of vertices, i.e. $D(g) = \max_{(i,j) \in N \times N} l_{ij}(g)$.

We denote the set of 'neighbors at distance k' of vertex i by $\Gamma_{i,k}(g)$, i.e., $\Gamma_{i,k}(g) = \{j \in N | l_{ij}(g) = k\}$

A hypergraph or affiliation network H is a pair (N, X), where N is a finite player set and $X \subset 2^N$ is a collection of subsets of N. Elements of X are called *events* or *cells*. We denote the set of cells a coalition of players $S \subset N$ is engaged in by $X(S) = \{A \in X | A \cap S \neq \emptyset\}$. The order of a hypergraph is the number of players $|N| = n$ and the size equals its number of cells $|X| = c$. The set of all subsets of N of size r is denoted by N^r. An $r-$uniform hypergraph on N is a pair (N, X) where $X \subset N^r$. The hypergraph (N, X) is connected if for every $i, j \in N$ there exists a sequence $A_1, ..., A_s$ of cells with $s \geq 1$, $A_l \in X$, for all $l \in \{1, ..., s\}$, such that $i \in A_1$, $j \in A_s$ and $A_t \cap A_{t+1} \neq \emptyset$ for $t = 1, ..., s-1$. The class of all connected hypergraphs with player set N is denoted by $\mathbb{C}(N)$. The class of connected affiliation networks in which each two cells have at most one player in common is denoted by $\mathbb{H}(N) = \{(N, X) \in \mathbb{C}(N) | \quad |A \cap B| \leq 1 \text{ for all } A, B \in X\}$. A cycle in a hypergraph $H = (N, X)$ is a sequence $A_1, ..., A_s$ with $s \geq 3$ of $s-1$ different cells $A_l \in X$, for all $l \in \{1, ..., s\}$, such that $A_i \cap A_{i+1} \neq \emptyset$ for $i = 1, ..., s-1$, $A_1 = A_s$ and $A_i \cap A_j = \emptyset$ otherwise. A connected hypergraph is a hypertree if it contains no cycles. We define the one-mode projection graph $g_\perp(H) = (N, E_H) \in \mathbb{G}(N)$ corresponding to the affiliation

network $H = (N, X) \in \mathbb{H}(N)$ by letting $ij \in E_H$ if and only if there exists an $A \in X$ such that $i, j \in A$.

A *cooperative transferable utility game* is an ordered pair (N, v) where $N = \{1, ..., n\}$ is a finite set of players and $v : 2^N \mapsto \mathbb{R}$ is a map assigning to each coalition $S \in 2^N$ a real number $v(S)$, called the worth of S, and where by convention $v(\{\emptyset\}) = 0$.

In cooperative game theory it is usually assumed that the grand coalition forms. Hence, one is interested in a division of the worth of the grand coalition. The *core* (cf. Gillies (1953)) of (N, v) is defined by

$$C(v) = \{x \in \mathbb{R}^N | \sum_{i \in N} x_i = v(N), x(S) \geq v(S) \text{ for all } S \subset N \text{ and } x(N) = v(N)\}$$

where $x(S) = \sum_{i \in S} x_i$. We may conclude that if $v(N)$ is divided according to a core-element, then no coalition has an incentive to split off from the grand coalition, since the total amount $x(S)$ is at most the worth $v(S)$ which coalition S can obtain by forming. The core can be an empty set. A cooperative game (N, v) is called *balanced* if $\sum_{S \subset N} \lambda(S) v(S) \leq v(N)$ for all functions $\lambda : 2^N \mapsto \mathbb{R}_+$ satisfying $\sum_{S \subset N : i \in S} \lambda(S) = 1$ for all $i \in N$. A game is called *totally balanced* if every subgame $(S, v|_S)$ is balanced. Bondareva [1963] and Shapley [1967] derived the following result about the core and balancedness.

Theorem 2.0.1 *(Bondareva, 1963; Shapley, 1967) Let (N, v) be a cooperative game. Then $C(v) \neq \emptyset$ if and only if (N, v) is balanced.*

Let $\Pi(N)$ be the set of all permutations of $N = \{1, ..., n\}$. Then the i-th coordinate of the *marginal vector* $m^\pi(v)$, $\pi \in \Pi(N)$, is defined by

$$m_i^\pi(v) = v(\{j \in N | \pi(j) \leq \pi(i)\}) - v(\{j \in N | \pi(j) < \pi(i)\}).$$

The Shapley value $\phi(v)$ [Shapley, 1953] of (N, v) is defined as the average of all marginal vectors, i.e.,

$$\phi(v) = \frac{1}{n!} \sum_{\pi \in \Pi(N)} m^\pi(v).$$

For each TU-game (N, v) we define the utopia payoff to player $i \in N$ by $M_i(v) = v(N) - v(N \setminus \{i\})$. Furthermore $m_i(v) = max\{v(S) - \sum_{j \in S \setminus \{i\}} M_j(v) | S \in 2^N, i \in S\}$ is the minimal right of player i. The compromise value for a game (N, v), introduced by Tijs [1981], is the efficient compromise between the utopia vector $M(v) \in \mathbb{R}^N$ and the minimum right vector $m(v) \in \mathbb{R}^N$, i.e., $\tau(v) = \alpha M(v) + (1 - \alpha) m(v)$.

Chapter 3

Homogeneous Covert Networks

'Never be afraid to try something new.
After all, a lone amateur built the Ark,
a team of experts built the Titanic.'
- Anonymous.

3.1 Introduction

Many countries in the world use covert operations as a means of leverage in exercising their power. For instance several thousand covert operations were mounted by the CIA and KGB during the Cold War. In part these operations consist of operating covert networks in non-friendly territory. Israel's operation Susannah, also known as the Lavon affair, is another case in point. Israel operated a covert network inside Egypt during the early 1950s. After activation the network was quickly detected and dismantled because the Egyptian intelligence service was able to find names of the accomplices of a suspect in the operation. This indicates that the social ties that exists in a covert organization present a potential hazard to the successful completion of an operation. Another example of a covert network that was exposed is the following. During the 1950's a group of lawyers and legal experts that turned against the communist regime in East Berlin were selected by the CIA to be converted to an underground armed resistance group consisting of cells of 3 individuals each [Weiner, 2007]. However, the network topology of this organization equalled that of a complete graph (the worst possible in the sense of secrecy) because all the individuals were acquainted with each other. Upon the exposure of one network member the Soviets discovered and arrested all the other members. The operation was a failure.

One traditional method to analyze social relationships among individuals is social network analysis. Recently an increasing interest in the application of methods from social network analysis to the study of covert organizations can be observed. For instance in counterinsurgency social network analysis is recognized to be one of the most important tools to describe effects of the operational environment and to evaluate the threat [Mishal and Rosenthal, 2005]. Moreover, it is realized that methods from several mathematical disciplines are valuable in analyzing covert networks. Sageman [2004] discusses the use of applying the network paradigm such as clustering and small-world phenomena to analyze terror networks . Social network analysis of specific terror events are available, although not abundant[Koschade, 2006].

Non-state actors also try to attain their goals in part by operating covertly. Several middle eastern organizations such as Hamas and Hezbollah not only consist of overt political parties participating in elections but also consist of covert security apparatuses designed to attain their policy goals by force. In addition, covert networks inside the Western world posed and still pose a challenge to the security environment by operating under a cloud of secrecy and deception. London's Metropolitan Police for instance became experts in counterterrorist operations during the Irish Republican Army 1970's terrorist campaign. Another more recent example is that of Al Qaeda. It is currently widely known that Al Qaeda morphed from a bureaucratic, hierarchical organization into an ideological umbrella for loosely coupled jihadi networks. We argue in this thesis that the changing environment pressured the Al Qaeda leadership into adopting network topologies that maintain secrecy while simultaneously providing some possibility to coordinate and control.

Considering this wide range of loose affiliates and organizations operating covert networks it is of utmost importance to analyze, understand and predict their topologies.

The sparse but important literature that deals with these kind of covert organizations characterize them as cellular organizations composed of quasi-independent cells and distributed command [Carley, 2006] and being organized decentralized rather than hierarchical [Tucker, 2001]. Formal characterizations of cellular networks exist [Tsvetovat and Carley, 2005], however a shortcoming of the literature on such networks is that it has been mostly of the historical case study and anecdotal variety [Asal et al., 2007] . It is also recognized that there are covert organizations that operate according to organizational structures that lie somewhere between hierarchical and completely decentralized [Mishal and Rosenthal, 2005].

In general it is stated that to coordinate successful policy to counter an enemy by outwitting and deceiving him first an endeavor to understand him must be undertaken [Creveld, 1991] . In the realm of terrorism this means that without a thorough understanding of the structure of terrorist organizations we remain unable to fulfill the most basic requirements of an effective counterterrorist strategy. Therefore, it is important to develop a general framework in which the structure of a covert network can be predicted and analyzed. What distinguishes covert organizations from 'normal' overt organizations? Baker and Faulkner discuss covert organizations and conclude that the requirement for secrecy distinguishes the covert organization from the overt organization: "every secret organization has to solve a fundamental dilemma: how to stay secret and at the same time ensure the necessary coordination and control of its members" [Baker and Faulkner, 1993], also see Raab and Brinton Milward [2001]. In a similar fashion McAllister [2004] notes that internal communication and coordination of a terrorist network preferably is organized according to an amorphous structure. Owen [2001] analyzes the tradeoff between operational efficiency and operational security of clandestine groups. Their focus among others is on optimizing group size, whereas the discussion on group structure focuses on the star and complete graph . Enders and Su [2007] analyze optimal network structures by modeling the tradeoff between security and intragroup communication with a focus on network density. Their approach explicitly models the strategic interaction between terrorists and government. However, their focus is on network *density* instead of structure per se. Other questions that are being raised concern covert network destabilizing strategies, see for instance Farley's work on breaking Al Qaeda cells [Farley, 2003] or Carley et al. [2003]. Social network analysis tools are also being applied in the study of covert networks. See for instance Koschade for a social network analysis of Jemaah Islamiyah's Bali bombing [Koschade, 2006] and Magouirk et al. [2008] for a more general discussion about Jemaah Islamiyah. Sparrow [1991] discusses the application of social network analysis to criminal intelligence and Kinsella [2005] for instance focuses on the small arms social networks. We will defer a more game theoretical discussion about this to chapter 7. In addition, criminal organizations have been analyzed focusing on the trade-off between diffusing information widely through the organization at the cost of leaving the organization more vulnerable to external threats [Bar-Isaac and Baccara, 2008].

It thus appears that a distinguishing factor between covert and overt organizations is the constant dilemma between secrecy and operational capability. It is known that terrorist organizations are aware of the importance of their network structure: in a video

lecture captured after the fall of Afghanistan in 2001 Mousab al Suri (also known as Mustafa Nasar the Syrian, an alleged Al Qaeda affiliate that was captured in November 2005) discusses the structure a covert organization should adopt [Bergen, 2006] . He indicates that certain network structures should be avoided to ensure the secrecy of the organization: "I advise your brigade doesn't exceed ten members. You shouldn't expand or form too many." [Cruickshank and Hage Ali, 2007]. Such considerations are also taken into account in the field of military swarming. Here units resemble an array of dispersed nodes set to act as an all-channel network. The challenge is to design military networks that depend on stealth and secrecy. In this case the three most common designs are the 'path' the 'star' and the 'complete' graph structure. However, Arquilla and Ronfeldt [2001] argue that hybrid forms are also good candidates .

To study how covert organizations deal with this dilemma one can either proceed from a practical/empirical approach or a theoretical approach. Considering the first approach some (but few) empirical observations indicate the influence of imposition of communication restrictions on efficient group performance, see for instance Bavelas [1948, 1950] or Guetzkow and Simon [1955]. However interesting, this work is hard to generalize since it is based on lab findings, considers only certain graphs of order 5 and analyzes a specific task to be completed by the group. There is a small body of empirical findings on the influence of social networks on team performance. For instance Baldwin [1997] found support for the premise that more ties are associated with enhanced team performance. Apart from anecdotal evidence no substantial research effort has been made to investigate this dilemma covert organizations face from observations or laboratory experiments. Clearly, in part this may be due to the nature of such networks since it is recognized that covert networks are often difficult to reason about due to the nature of data available on these systems [Carley, 2006]. In addition explicit topologies of covert networks, based on theoretical considerations, are usually not provided. Hence the other approach, deductive reasoning to obtain insight into the dilemma of secrecy and operational efficiency covert organizations face, is valuable.

In this chapter, based on Lindelauf et al. [2009a], we analyze the problem of covert network structure design taking the above mentioned dilemma explicitly into account from a theoretical perspective. The strategic interaction between a covert organization and its opposing forces is modeled by the assumption that secrecy is a key design parameter. We consider both secrecy and information processing efficiency as key network design parameters and we analyze several different scenarios corresponding to different assumptions on those parameters. Implicit in this approach is the assumption that the

covert group is willing to adopt that network structure that optimizes the tradeoff between secrecy and operational efficiency, and thus not necessarily maximizes individual incentives. Our approach is distinct from, though appears related to, the so-called degree/diameter problem that arises in graph theory: what is the largest number of nodes in a network with a limited degree and diameter? For an overview of results on this problem for instance see [Miller and Siran, 2005] . We will briefly discuss this topic in Section 3.4.1.

The first scenario corresponds to the situation of a covert operation in its initial phase in a hostile environment. We assume that it is equally likely for network members to be exposed and upon exposure of an individual all direct communication of this individual with others is detected. In the second scenario we assume that an initial operation is conducted in an environment of varying hostility. That is, we assume that there is a certain fixed probability that communication of any exposed individual with others is intercepted. Finally, we consider the scenario of a covert operation in a hostile environment that passed its initial stage. That is, we assume that exposure of an individual depends on his centrality with regard to information exchange and upon exposure all his communication with others is detected.

The relationships between individuals in a covert organization are modeled as a graph. A vertex can be interpreted as either an individual, a terrorist cell or a military unit. In the latter two cases we view a cell (or unit) as a single operational entity and we are interested in the communication structure among cells (units). There exists an edge between two individuals whenever there is an exchange of information between the corresponding vertices on a regular basis. The exchange of information for instance may represent the fact that one individual facilitates weapons or false documents to another, or it may represent target selection information exchange between differing cells. The underlying idea is that for the covert organization to execute a mission successfully cooperation and coordination are necessary.

Secrecy will be defined by using two parameters: the exposure probability and the link detection probability. In different scenarios these parameters will be varied. As a first approach in modeling the possibilities for communication of individuals in the organizations an information measure is defined in two ways based on the physical reach of information. First the average distance is used in defining the network performance in the sense of information. Second, to check robustness of the results, a worse-case performance bound of information exchange is taken by modeling the information measure using the

diameter of the underlying graph. Under the assumption of uniform exposure probability of network members (an operation in its initial stage) we will show that either the all-to-all graph or star graph is the optimal design solution, depending on the link detection probability. We show that cellular networks are optimal if the exposure probability of network members depends on the network structure. Finally we present a first approach to analyze optimal network structures taking into account that some organizations value secrecy much more than information as design parameter and vice versa.

In Section 3.2 preliminaries on the total distance in standard graphs will be discussed. The tradeoff between information and secrecy, and the corresponding Nash bargaining problem, will be discussed in Section 3.3. In Section 3.4 (approximate) optimal covert networks will be established for several different scenarios regarding secrecy. To indicate the robustness of the results a variation on the information measure and its corresponding optimal networks will be discussed in Section 3.5. Section 3.6 shortly discusses how to analyze optimal structures when placing much more emphasis on secrecy or information respectively. Section 3.7 the concludes this chapter.

3.2 Total distance and a diameter of a graph

Remember that the total distance $T(g)$ in the graph $g = (N, E)$ is defined by $\sum_{i,j} l_{ij}(g) = \sum_{i \in N} \sum_{j \in N} l_{ij}(g)$. Here we compute the total distance of the standard graphs g^n_{star}, g^n_{ring}, g^n_{path} and g^n_{comp} (see Figure 2.1 for these graphs of order 5).

	$T(g)$	$D(g)$
g^5_{star}	32	2
g^5_{ring}	30	2
g^5_{path}	40	4
g^5_{comp}	20	1

Table 3.1: Total distance and diameter for several order 5 graphs

We list the total distance and diameter of each graph in Table 3.1. For instance, the star graph g^5_{star} has one vertex with distance 1 to all the other vertices (the center vertex) and all other vertices have distance 1 to the center vertex and distance 2 to the remaining three vertices. Therefore $T(g^5_{star}) = 4 + 4(1 + 2 \cdot 3) = 32$. Clearly, the maximum of the

geodesic distances in the star graph equals 2: $D(g^5_{star}) = 2$.
For the four standard types of graphs the total distances are provided in Lemma 3.2.1.

Lemma 3.2.1

(i) $T(g^n_{star}) = 2(n-1)^2$

(ii) $T(g^n_{ring}) = \begin{cases} \frac{n^3-n}{4} & \textit{if } n \textit{ is odd} \\ \\ \frac{n^3}{4} & \textit{if } n \textit{ is even} \end{cases}$

(iii) $T(g^n_{path}) = \frac{(n-1)n(n+1)}{3}$

(iv) $T(g^n_{comp}) = n(n-1)$

Proof:

(i) Denote the center vertex of g^n_{star} with index c. Clearly $\sum_{i\in N} l_{ci}(g^n_{star}) = n-1$. For $j \in N$, $j \neq c$ $\sum_{i\in N} l_{ji}(g^n_{star}) = 1 + 2(n-2) = 2n-3$. Therefore $T(g^n_{star}) = \sum_{i\in N}\sum_{j\in N} l_{ij}(g^n_{star}) = n-1+(n-1)(2n-3) = 2(n-1)^2$.

(ii) First consider the case when n is odd. Then for all $i \in N$: $\sum_{j\in N} l_{ij}(g^n_{ring}) = 2(1+2+...+\frac{n-1}{2}) = \frac{(n-1)(n+1)}{4}$. Hence, $T(g^n_{ring}) = \frac{(n-1)n(n+1)}{4}$ for the case that n is odd. In case n is even it follows that for all $i \in N$: $\sum_j l_{ij}(g^n_{ring}) = 2(1+2+...+(\frac{n}{2}-1))+\frac{n}{2} = \frac{n^2}{4}$. Therefore $T(g^n_{ring}) = \frac{n^3}{4}$ in case n is even.

(iii) There are $n-1$ tuples $\{i,j\}$ such that $l_{ij}(g^n_{path}) = 1$, $n-2$ tuples $\{i,j\}$ such that $l_{ij}(g^n_{path}) = 2$,..., 1 tuple $\{i,j\}$ such that $l_{ij}(g^n_{path}) = n-1$. Each tuple has to be counted twice, therefore

$$\begin{aligned} T(g^n_{path}) &= 2\{(n-1)+2(n-2)+3(n-3)+...+(n-1)(n-(n-1))\} \\ &= 2\{n+2n+3n+...+(n-1)n-(1+2^2+3^2+...+(n-1)^2)\} \\ &= 2\{n\cdot\sum_{k=1}^{n-1}k-\sum_{k=1}^{n-1}k^2\} \\ &= 2\{\frac{n\cdot n(n-1)}{2}-\frac{(n-1)n(2n-2+1)}{6}\} \\ &= \frac{(n-1)n(n+1)}{3} \end{aligned}$$

(iv) For all $i \in N$ it holds that $\sum_{j\in N} l_{ij}(g^n_{comp}) = n-1$. Thus $T(g^n_{comp}) = n(n-1)$. □

3.3 The Tradeoff between Information and Secrecy

Usually in graphs the time delay for sending information from one vertex to the other is assumed to be proportional to the number of edges the information must travel. Such a graph may for instance represent a telecommunications network, a multiprocessor or local area network. The same holds for covert networks. In covert networks however the higher the number of edges a 'message' must travel the more likely it becomes that it will be intercepted. The information measure $I(g)$, of a covert network $g \in \mathbb{G}^n$ is therefore defined by the (normalized) reciprocal of the total distance,

$$I(g) = \frac{n(n-1)}{T(g)}.$$

Since $T(g) \geq n(n-1)$ for any $g \in \mathbb{G}^n$ it follows that $0 \leq I(g) \leq 1$. If $I(g) > I(g')$, then in network g it is easier (in an average sense) to send information around than in network g'. If everybody is able to communicate with everybody else, information can flow freely which gives the best information performance: $I(g^n_{comp}) = 1$.

Example 3.1:
Consider the complete graph g^5_{comp}, the star graph g^5_{star}, the path graph g^5_{path} and the ring graph g^5_{ring} as in Figure 2.1. It follows that $I(g^5_{comp}) = 1$, $I(g^5_{star}) = \frac{5}{8}$, $I(g^5_{path}) = \frac{1}{2}$ and $I(g_{ring}) = \frac{2}{3}$. Thus we have, $I(g^5_{comp}) > I(g^5_{ring}) > I(g^5_{star}) > I(g^5_{path})$. $\diamond$

The performance of the network $g = (N, E)$ in sense of secrecy will be indicated by $S(g)$. We assume that there are two factors for each individual in the network that contribute to this secrecy. Consider for instance the case of Nawaf al Hazmi, selected by Bin Laden as one of the suicide operatives for the 9-11 operation. As discussed in the 9-11 Commission Report: "U.S. intelligence would analyze communications associated with Midhar whom they identified during this travel, and Hazmi, whom they could have identified but did not." [Kean et al., 2002] . Thus first, there is a certain probability $\alpha_i(g)$ that upon surveillance individual i will be exposed as member of the network, and second if i is detected he will expose a fraction of the network which is represented by $1 - u_i(g)$. We assume that $\sum_{i \in N} \alpha_i(g) = 1$, i.e., $\alpha_i(g)$ represents the probability that individual i will be exposed conditioned on the fact that one individual will be exposed.

We define the secrecy measure $S(g)$ by

$$S(g) = \sum_{i \in N} \alpha_i(g) u_i(g)$$

where u_i reflects the fraction of the network that remains unexposed when i is detected. This measure thus reflects the expected fraction of the network that remains undetected. Furthermore we define,

$$\mu(g) = S(g)I(g) \tag{3.1}$$

as a total performance measure or criterion to compare graphs. A motivation for this choice is provided below.

In setting up a covert network conflicting objectives arise. First, the danger of exposure should be minimized and second, sufficient communication possibilities between members should exist. This situation can be modeled by an imaginative bargaining situation over the set of all possible connected networks where the secrecy measure corresponds to one preference and the information measure to another. The bargaining will eventually result in a network structure that in some sense fulfills the desire in having 'sufficient' secrecy and information capabilities. This approach differs from traditional network formation models where equilibrium requirements are analyzed such that individuals do not benefit from altering the structure of the network. In those models network formation is considered to be a local process, i.e., the breaking or forming of a link between two individuals depends on the change in payoff for the respective individual, not on the change in payoff for the network as a whole [Jackson, 2008]. Individuals form or break links according to some local criterion. Here instead we consider the formation of a network in such a way that all individuals are willing to adopt a global network structure that is optimal (in a bargaining sense) in the possibility to coordinate while maintaining secrecy.

The approach to determine which network structure will be adopted thus consists of assigning a secrecy and information measure to each network and then select that network structure that best satisfies these conflicting objectives. Such multiple conflicting objectives arise often in real-world optimization problems. Think of optimization of fuel efficiency, payload and weight in aerospace engineering or low mass and high stiffness objectives in mechanical engineering. Common solutions to these kind of problems consist of looking at a certain subset of the design space (often the Pareto set) or to optimize a single (heuristic) objective function [Siarry, 2003]. By demanding certain properties (such as Pareto optimality) of the covert network design solution we arrive at a single objective function as follows. We model the problem of finding an optimal graph of given order by analyzing the tradeoff between secrecy and operational efficiency as a finite Nash bargaining problem.

A two-person finite bargaining problem is a pair $(F, 0)$ where $F \subset \mathbb{R}^2$ is a finite set of feasible outcomes and $0 \in F$ represents the disagreement point. The disagreement point is the value the players can expect to recept if no bargain can be reached. Let $\mathbb{B}$ denote the class of all finite bargaining problems of this type. In our setting the set of feasible outcomes equals $F_* \equiv \{(S(g), I(g))|g \in \mathbb{G}^n\}$, where each point $(S, I) \in F_*$ corresponds to those graphs $g \in \mathbb{G}^n$ with secrecy measure $S(g) = S$ and information measure $I(g) = I$. A bargaining solution ϕ assigns to each $(F, 0) \in \mathbb{B}$ a non empty subset $\phi((F, 0))$ of F. The Nash bargaining solution, $N(F, 0)$, is defined by

$$N(F, 0) = argmax \quad \{x_1 x_2 | x = (x_1, x_2) \in F\} \quad \text{for all } (F, 0) \in \mathbb{B}.$$

In our application the Nash bargaining solution will lead to those graphs that maximize the product of secrecy and information measure, that is

$$N(F_*, 0) = argmax \quad \{\mu(g) = S(g)I(g) | g \in \mathbb{G}^n\}.$$

The Nash bargaining solution can be motivated on the basis of the following general properties which have a strong appeal in our application framework. A bargaining solution ϕ satisfies

1. Weak Pareto Optimality: For all $x = (x_1, x_2) \in \phi((F, 0))$: if $t = (t_1, t_2)$ such that $t_1 > x_1$ and $t_2 > x_2$, then $t \notin F$

2. Symmetry: Let F be such hat for all $(x_1, x_2) \in F$ it also holds that $(x_2, x_1) \in F$. Then $(x_1, x_2) \in \phi((F, 0))$ implies $(x_2, x_1) \in \phi((F, 0))$.

3. Independence of Irrelevant Alternatives: If $F \subset G$ and $\phi(G) \cap F \neq \emptyset$, then $\phi(F) = \phi(G) \cap F$.

4. Covariance with positive scale transformations: Let $\tau : \mathbb{R}^2 \mapsto \mathbb{R}^2$ be a positive linear transformation given by $\tau(x) = (\lambda_1 x_1, \lambda_2 x_2)$, with $\lambda_1, \lambda_2 > 0$, for all $x = (x_1, x_2) \in \mathbb{R}^2$. Then $\phi(\tau(F)) = \tau(\phi(F))$.

The first property, called *Weak Pareto Optimality* (WPO) , translated to our framework, states that for any 'optimal graph' there can not be another graph which has both a higher secrecy measure and information measure. The second property of *Symmetry* (SYM) simply states that the secrecy measure and information measure are equally relevant. This assumption can be relaxed if one considers organizations that value secrecy (resp. information) much more than information (resp. secrecy). In that case the Nash bargaining solution can be parameterized by α such that it becomes $\mu(g) = S^\alpha(g) I^{1-\alpha}(g)$.

In Section 2.6 we provide an initial analysis of network optimality for all three scenarios depending on the value of α. The third property, *Independence of Irrelevant Alternatives* (IIA) , states that if the set of networks about which the agents bargain is reduced, those solutions of the larger bargaining problem that are still available should form the solutions of the smaller bargaining problem. The final property, *covariance with positive scale transformations* (COV), states that a positive scaling of the secrecy and information measure (i.e., changing units of measurement) re-scales the bargaining outcome in the corresponding way. In fact, the Nash bargaining solution is characterized by the above four properties:

Theorem 3.3.1 *[Mariotti, 1998] Let ϕ be a bargaining solution on $\mathbb{B}$. Then $\phi = N(F, 0)$ if and only if ϕ satisfies WPO, SYM, IIA and COV.*

3.4 Optimal Structures of Covert Networks

In this section we analyze several different scenarios and present network design solutions for each. In Section 3.4.1 it is assumed that individuals in the network are exposed uniformly and that upon exposure of an individual all his links with other members are detected. The main result under those assumptions is that the network's optimal structure is that of a star graph.

In Section 3.4.2 it is assumed that with probability p communication over a link will be detected independently and identically for all links. It will be shown that the optimal network structure will be that of the complete graph for low values of p, and the star graph for high values of p, extending the result of Section 3.4.1. Finally, in Section 3.4.3 it is shown that if the network structure is taken into account in defining the exposure probability of individuals and that if upon exposure all links of this individual are detected the resulting optimal network structures are cellular. Exact results are given for $n \leq 7$ and heuristic algorithms are developed to analyze higher order graphs.

3.4.1 Scenario 1: Detecting all links of an exposed individual

Initially we define the secrecy individual i 'contributes' to the network as the fraction of individuals that remain unexposed when upon monitoring individual i all his links with his neighbors are detected. That is, for $g \in \mathbb{G}^n$

$$u_i(g) = 1 - \frac{d_i(g) + 1}{n}.$$

Moreover we set $\alpha_i = \frac{1}{n}$. That is, we assume that individuals are uniformly exposed as being a member of the network.
Let $g \in \mathbb{G}(n,m)$. It follows from the definition of the secrecy measure that (using subscript 1 to explicitly denote the scenario),

$$S_1(g) = \frac{1}{n}\sum_{i\in N} u_i(g) = \frac{n^2-n-2m}{n^2}.$$

With $I(g) = \frac{n(n-1)}{T(g)}$ reflecting the average (information) measure of g and

$$\mu_1(g) = S_1(g)I(g),$$

we derive that,

$$\mu_1(g) = \frac{n^2-n}{n^2}\cdot\frac{n^2-n-2m}{T(g)}. \tag{3.2}$$

Example 3.2:
Reconsider the graphs of Figure 2.1. The values for the secrecy measure, information measure and total performance measure of order 5 graphs corresponding to the first scenario are given in Table 3.2 below. ◇

	$S_1(g)$	$I_1(g)$	$\mu_1(g)$
g^5_{star}	$\frac{12}{25}$	$\frac{5}{8}$	$\frac{3}{10}$
g^5_{ring}	$\frac{10}{25}$	$\frac{2}{3}$	$\frac{4}{15}$
g^5_{path}	$\frac{12}{25}$	$\frac{1}{2}$	$\frac{6}{25}$
g^5_{comp}	0	1	0

Table 3.2: Secrecy, information and total performance measure of order 5 graphs, scenario 1.

We will show that no graph of order n performs better than g^n_{star}. To do this we first derive a lower bound for the total distance $T(g)$.

Lemma 3.4.1 *Let $g \in \mathbb{G}(n,m)$. Then $T(g) \geq 2n(n-1) - 2m$.*

Proof:
Since g has size m, there are exactly m tuples $\{i,j\}$ of vertices for which $l_{ij} = 1$. For all other $\frac{n(n-1)}{2} - m$ tuples $\{i,j\}$ it holds that $l_{ij} \geq 2$. Hence $T(g) \geq (m + 2(\frac{n(n-1)}{2} - m))\cdot 2 = 2n(n-1) - 2m$. □

Theorem 3.4.1 *$\mu_1(g^n_{star}) \geq \mu_1(g)$ for all $g \in \mathbb{G}^n$.*

Proof:
Suppose there exists a $g \in \mathbb{G}(n,m)$ such that $\mu_1(g) > \mu_1(g^n_{star})$.
Then $\frac{n^2-n-2m}{T(g)} > \frac{n-2}{2(n-1)}$ or equivalently, $T(g) < (2n(n-1)-4m)\frac{n-1}{n-2}$.
However, one readily checks that $(2n(n-1)-4m)\frac{n-1}{n-2} \leq 2n(n-1)-2m$.
Hence, $T(g) < 2n(n-1)-2m$, contradicting Lemma 3.4.1. □

3.4.2 Scenario 2: Detecting links with fixed probability

In this subsection we assume that whenever an individual in the network is being monitored communication between him and one of his neighbors is detected independently with probability p. The case where $p = 1$ therefore corresponds to the first scenario as analyzed in the previous section. If individual i has $d_i(g)$ neighbors the number of neighbors that will be detected is binomially distributed. Consequently we define,

$$u_i(g) = 1 - \frac{pd_i(g)+1}{n}$$

and again assume $\alpha_i = \frac{1}{n}$. Therefore we have, for $g \in \mathbb{G}(n,m)$

$$S_2(g) = \frac{n^2-n-2pm}{n^2}.$$

With $I(g)$ as before we find

$$\mu_2(g) = S_2(g)I(g) = \frac{n^2-n}{n^2} \cdot \frac{n^2-n-2pm}{T(g)}. \tag{3.3}$$

For low values of p the complete graph maximizes μ_2.

Theorem 3.4.2 *If $p \in [0, \frac{1}{2}]$, then $\mu_2(g^n_{comp}) \geq \mu_2(g)$ for all $g \in \mathbb{G}^n$.*

Proof:
Note that $T(g_{comp}) = n(n-1)$ and hence $\mu_2(g^n_{comp}) = \frac{n^2-n}{n^2} \cdot (1-p)$. Suppose there exists a $g \in \mathbb{G}(n,m)$ such that $\mu_2(g) > \mu_2(g^n_{comp})$ then $\frac{n^2-n-2pm}{T(g)} > (1-p)$, or equivalently $T(g) < \frac{n^2-n-2pm}{1-p}$. However, one readily checks that for all $p \in [0, \frac{1}{2}]$ $\frac{n^2-n-2pm}{1-p} \leq 2n(n-1)-2m$.
Hence $T(g) < 2n(n-1)-2m$, contradicting Lemma 3.4.1. □

For high values of p we extend the result of the previous section ($p = 1$).

Theorem 3.4.3 *If* $p \in [\frac{1}{2}, 1]$, *then* $\mu_2(g^n_{star}) \geq \mu_2(g)$ *for all* $g \in \mathbb{G}^n$.

Proof:
Note that $T(g^n_{star}) = 2(n-1)^2$ and $\mu_2(g^n_{star}) = \frac{n^2-n}{n^2} \cdot \frac{n-2p}{2(n-1)}$. Suppose there exists a $g \in \mathbb{G}(n,m)$ such that $\mu_2(g) > \mu_2(g^n_{star})$. Then $\frac{n^2-n-2pm}{T(g)} > \frac{n-2p}{2(n-1)}$ or equivalently $T(g) < \frac{2(n-1)(n^2-n-2pm)}{n-2p}$. For $p \in [\frac{1}{2}, 1]$ however, it is readily verified that $\frac{2(n-1)(n^2-n-2pm)}{n-2p} \leq 2n(n-1) - 2m$, contradicting Lemma 3.4.1. □

In case $p = \frac{1}{2}$ it follows from Theorem 3.4.2 and Theorem 3.4.3 that μ_2 is maximal for both g_{star} and g_{comp}. However, for $p = \frac{1}{2}$ it is not the case that all graphs maximize μ_2: $\mu_2(g^5_{comp}) = \mu_2(g^5_{star}) = \frac{10}{25}$ whereas $\mu_2(g^5_{ring}) = \frac{8}{25}$.

As an illustration consider the network structure of the former Dutch National Clandestine Service's so-called 'stay behind organization'. After the Second World War it was decided that precautionary measures should be taken such that in the event of a sudden invasion of the Netherlands a covert organization would be present to assist in subversive and covert activities to support the overthrow of the occupying forces[Engelen, 2005]. This covert organization was divided into two groups: group A and B. Support group 'A' consisted of single agents all equipped with radio systems to connect to the Allied Clandestine Base (ACB). These single agents were not aware of each other because the chosen network structure equalled that of a star graph. Due to the extreme covert nature of this network (which was finally disbanded after the end of the Cold War in 1992) the initial exposure probability of network members may be assumed to be uniform. Communicating with the ACB presented a high link detection probability (high value for p) hence it can be argued that the star network design was an optimal choice. However, after operating for an extended period of time the exposure probability of the single agents would not be uniform anymore but would start to depend on their 'activity' in exchange of information.

3.4.3 Scenario 3: Non-uniform exposure probability

Up to now we assumed that $\alpha_i = \frac{1}{n}$ for all $i \in N$. It can be argued that this is the case when a covert operation is in its initial phase. However, if an operation passed its initial stage the probability of exposure will vary among network members. This because certain individuals, due to a more central position in the network, are more likely to be

discovered. We model this 'information centrality' by the equilibrium distribution of a random walk on the graph. This random walk chooses its next vertex at uniformly at random from the neighbors of the current vertex including itself. For $g \in \mathbb{G}(n,m)$, the equilibrium distribution is denoted by $\pi = (\pi_1, ..., \pi_n)$ and is given by $\pi_i = \frac{d_i(g)+1}{2m+n}$, see for instance Tijms [2003]. We set $\alpha_i = \pi_i$ and choose,

$$u_i(g) = 1 - \frac{d_i(g)+1}{n}$$

It follows that

$$\begin{aligned} S_3(g) &= \sum_{i \in N} \pi_i u_i(g) \\ &= \frac{2m(n-2) + n(n-1) - \sum_{i \in N} d_i(g)^2}{(2m+n)n}. \end{aligned}$$

With

$$I(g) = \frac{n(n-1)}{T(g)}$$

we derive

$$\mu_3(g) = \frac{(n-1)}{2m+n} \cdot \frac{2m(n-2) + n(n-1) - \sum_{i \in N} d_i(g)^2}{T(g)}. \tag{3.4}$$

We obtain explicit expressions of equation μ_3 for the standard graphs. The proof is straightforward (using Lemma 3.2.1), and therefore omitted.

Theorem 3.4.4

(i) $\mu_3(g^n_{comp}) = 0$;

(ii) $\mu_3(g^n_{star}) = \frac{n-2}{3n-2}$;

(iii)

$$\mu_3(g^n_{ring}) = \begin{cases} \frac{4(n-1)(n-3)}{n^3} & \text{if } n \text{ is even,} \\ \frac{4(n-3)}{n(n+1)} & \text{if } n \text{ is odd;} \end{cases}$$

(iv) $\mu_3(g^n_{path}) = \frac{3(n-2)(3n-5)}{n(3n-2)(n+1)}$.

Comparing the expressions provided in Theorem 3.4.4 we obtain

Corollary 3.4.1

(i) $\mu_3(g^4_{path}) > \mu_3(g^4_{star}) > \mu_3(g^4_{ring}) > \mu_3(g^4_{comp})$

(ii) $\mu_3(g^5_{ring}) > \mu_3(g^5_{path}) = \mu_3(g^5_{star}) > \mu_3(g^5_{comp})$

(iii) $n = \{6, 7, 8\}$*:* $\mu_3(g^n_{ring}) > \mu_3(g^n_{star}) > \mu_3(g^n_{path}) > \mu_3(g^n_{comp})$

(iv) $n = \{9, ...\}$*:* $\mu_3(g^n_{star}) > \mu_3(g^n_{ring}) > \mu_3(g^n_{path}) > \mu_3(g^n_{comp})$

The graphs $g \in \mathbb{G}^n$ that maximize $\mu_3(g)$ for $n = 2, ..., 7$ are shown in Figure 3.1. It

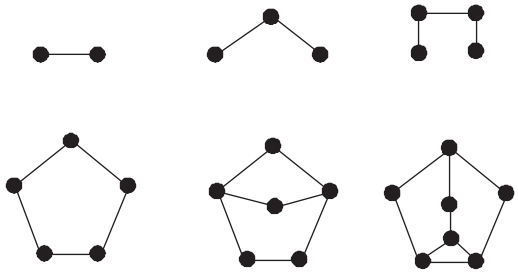


Figure 3.1: Optimal graphs for scenario 3 for $n \in \{2, ..., 7\}$, with average information measure.

can be seen that the optimal networks adopt a cellular structure. For large values of n it is not possible to calculate exact solutions and we resort to a simulation technique. We provide two algorithms to approximate the graph that maximizes μ_3. The first algorithm (I) randomly generates a graph. Each edge is present with probability $\frac{1}{2}$. If the resulting graph g is connected $\mu_3(g)$ is computed and stored. Next another graph g' is generated and $\mu_3(g')$ is compared to $\mu_3(g)$. If $\mu_3(g') > \mu_3(g)$ the graph g is replaced by g'. If not, g is kept. This process is iterated for 500.000 times.

The second algorithm (II) is local in nature. The starting point is a connected graph g of small size (a tree or a ring graph for instance) for which $\mu_3(g)$ is computed. Next edges are randomly added one by one as long as this increases the value of μ_3. The algorithm ends when adding a single edge does not increase the value of μ_3. Different starting graphs may result in different outcomes. Therefore several starting graphs are tried and the one yielding the graph g' with maximum $\mu_3(g')$ is selected. Finally, the outcomes of algorithm I and II are compared and the graph with the highest value for μ_3 is selected as the approximate solution for our μ_3 maximization problem.

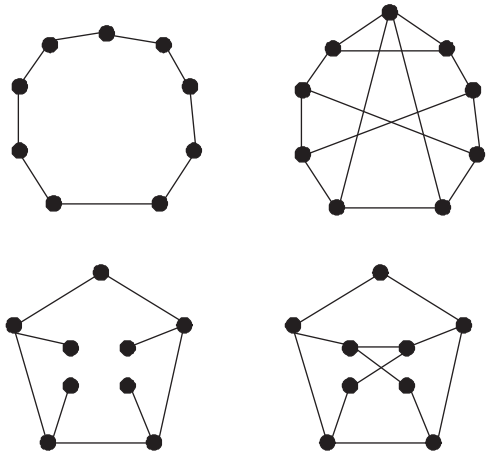


Figure 3.2: Local optimization starting graphs (top left and down left) and their resulting approximate optimal graphs (top right and down right respectively).

Example 3.3:
Consider $n = 9$. Using algorithm I we generated and compared 500.000 connected graphs yielding the best graph shown in Figure 3.2 above (down right) with a total performance measure of 0.3348. The second algorithm was run starting from several different small order graphs of which two are shown in the same figure. Local optimization starting from the down left tree resulted in the down right graph, the same as resulted from algorithm I. Starting algorithm II from the top left graph resulted in the graph g shown in the top right, for which $\mu_3(g) = 0.3355$. Actually, using other initial graphs did not yield a graph with a higher value of μ_3. ◇

In Figure 3.3 we present the results of this process for graphs of order $n = 8, 9$, and 10 respectively. It can be seen that for $n = 10$ the Petersen graph appears to approximate the optimal one. It should be noted that the Petersen graph is a special kind of graph that appears prominently in the so-called degree/diameter problem [Miller and Siran, 2005] : given natural numbers Δ and D, find the largest possible number of vertices $n_{\Delta,D}$ in a graph of maximum degree Δ and diameter $\leq D$. Trivially $\Delta = 1$ implies $D = 1$ hence $n_{1,1} = 2$. A straightforward upper bound, the so-called Moore bound $M_{\Delta,D}$, for $n_{\Delta,D}$ equals

$$n_{\Delta,D} = \begin{cases} 1 + \Delta\frac{(\Delta-1)^D-1}{\Delta-2} & \text{if } \Delta > 2 \\ \\ 2D+1 & \text{if } \Delta = 2 \end{cases}$$

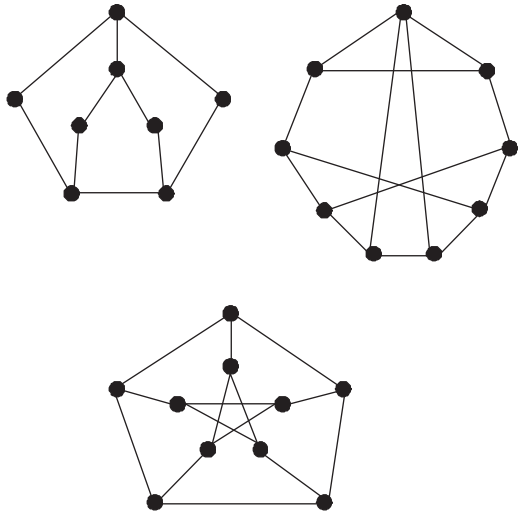


Figure 3.3: Approximate optimal graphs for scenario 3, of order 8,9 and 10.

A pioneering paper of Hoffman and Singleton was devoted to graphs of diameter 2 and 3 that attained the Moore bound [Hoffman and Singleton, 1960] . They proved that Moore graphs exist for $\Delta = 2, 3, 7$ and possible 57 but for no other degrees. In addition they showed that for the first three values of Δ the graphs are unique, being g^5_{ring} in case of $\Delta = 2$, the Petersen graph for degree $\Delta = 3$ and the Hoffman-Singleton graph for degree $\Delta = 7$ (see Figure 3.3). Comparing these to the optimal graphs in the third scenario it turns out that in case of $n = 5$ our optimal graph coincides with the Moore graph of order $n = 5$. In addition it appears that the Petersen graph maximizes μ_3 in case of $n = 10$. Whether or not the Hoffman-Singleton graph is also optimal in case of $n = 50$ is still an open question. Finally Figure 3.4 depicts approximate optimal graphs for some larger values of n: $n = 25$ and $n = 40$.

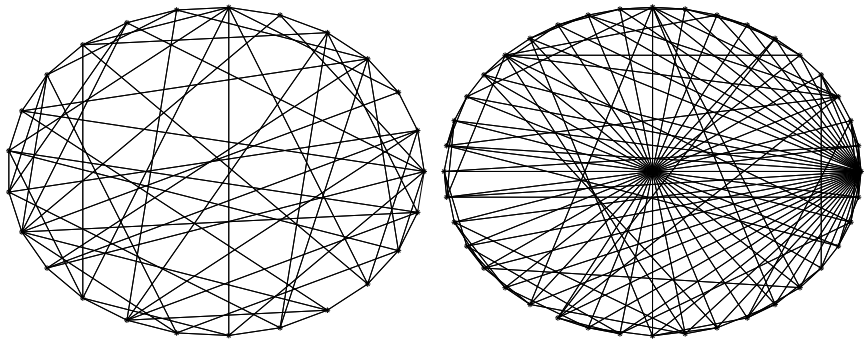


Figure 3.4: Approximate optimal graphs for scenario 3, for n=25 (left) and n=40 (right), average information measure.

It can be seen that for $n = 25$ a cellular structure emerges. The degree varies between 5 and 7. For the approximate optimal graph of order 40 also cellular structures appear but now it can be seen that a central individual emerges (not connected to everyone but with high degree) around which smaller cells are distributed.

3.5 A Variation on the Information Measure

The analysis so far has been conducted with information performance measured by the (normalized) reciprocal of the total distance in the network. This information measure represented the *average* performance of the network with respect to the exchange of information. Here we repeat the analysis, using an information measure taking worst case performance into account. Actually, in considering problems in communication over networks or circuit layout optimization often the diameter is considered to be the decisive parameter[Chung, 1987]. We define the worst case performance information measure $\overline{I}(g)$ by

$$\overline{I}(g) = \frac{1}{D(g)}. \tag{3.5}$$

We use the upper bar to explicitly differentiate this measure from the information measure used before. Obviously $0 \leq \overline{I}(g) \leq 1$ and $\overline{I}(g_{comp}) = 1$. Moreover, if $\overline{I}(g) > \overline{I}(g')$, then worst case performance in g is better than in g'.

First consider scenario 1: uniform exposure probability and detection of all links. For $g \in \mathbb{G}(n, m)$ with,

$$S_1(g) = \frac{n^2 - n - 2m}{n^2}$$

and $\overline{I}(g)$ as in equation (3.5) we have,

$$\overline{\mu}_1(g) = S_1(g)\overline{I}(g) = \frac{n^2 - n - 2m}{D(g)n^2}. \tag{3.6}$$

It turns out that g^n_{star} maximizes $\overline{\mu}_1$ over $\mathbb{G}^n$.

Theorem 3.5.1 *For all $g \in \mathbb{G}^n$, $\overline{\mu}_1(g^n_{star}) \geq \overline{\mu}_1(g)$*

Proof:
Let $g \in \mathbb{G}(n,m)$. Clearly $m \geq n-1$ (we only consider connected graphs). With $\overline{\mu}_1(g^n_{star}) = \frac{(n-1)(n-2)}{2n^2}$ it follows readily that $\overline{\mu}_1(g) > \overline{\mu}_1(g_{star})$ implies $D(g) < 2$. This however would lead to $D(g) = 1$ and thus $g = g_{comp}$. Since $\overline{\mu}_1(g_{comp}) = 0$ we arrive at a contradiction. □

Next we consider scenario 2 with a probability p of link detection, again assuming uniform exposure of individuals. Using the worst case performance information measure $\overline{I}(g)$ and secrecy measure

$$S_2(g) = \frac{n^2 - n - 2pm}{n^2}$$

we have for all $g \in \mathbb{G}(n,m)$,

$$\overline{\mu}_2(g) = S_2(g)\overline{I}(g) = \frac{n^2 - n - 2pm}{D(g)n^2} \tag{3.7}$$

Theorem 3.5.2 *For all $g \in \mathbb{G}^n$ and all $p \in [0,1]$, we have,*

(i) $\overline{\mu}_2(g^n_{comp}) \geq \overline{\mu}_2(g)$ *if* $p \leq \frac{n}{2(n-1)}$

(ii) $\overline{\mu}_2(g^n_{star}) \geq \overline{\mu}_2(g)$ *if* $p \geq \frac{n}{2(n-1)}$

Proof:
If $g \in \mathbb{G}^n$ is such that $\overline{\mu}_2(g) > \overline{\mu}_2(g_{star})$ then $D(g) = 1$ and consequently $g = g^n_{comp}$. Note that $\overline{\mu}_2(g_{comp}) = \frac{(n^2-n)(1-p)}{n^2}$ and $\overline{\mu}_2(g_{star}) = \frac{n^2-n(1+2p)+2p}{n^2}$. Therefore $\overline{\mu}_2(g^n_{comp}) \geq \overline{\mu}_2(g^n_{star})$ if and only if $p \leq \frac{n}{2(n-1)}$. □

Finally we analyze scenario 3 (non-uniform exposure probability). With secrecy measure for $g \in \mathbb{G}(n,m)$ given by

$$S_3(g) = \frac{2m(n-2) + n(n-1) - \sum_{i \in N} d_i^2}{(2m+n)n}$$

it follows that

$$\overline{\mu}_3(g) = S_3(g)\overline{I}(g) = \frac{2m(n-2) + n(n-1) - \sum_{i \in N} d_i^2}{D(g)(2m+n)n} \tag{3.8}$$

The graphs $g \in \mathbb{G}^n$ that maximize $\overline{\mu}_3$ for $n \in \{2, ..., 7\}$ are provided in Figure 3.5. It can be seen that the optimal graphs are similar to those for scenario 3 with $I(g) = \frac{n(n-1)}{T(g)}$ (see Figure 3.1). Only the optimal graph of order $n = 4$ is different. This shows the robustness of our results in case of lower order graphs.

Finally approximate optimal graphs for larger orders are presented in Figure 3.6, using the same approximation technique as explained in the Section 3.4. For the left graph

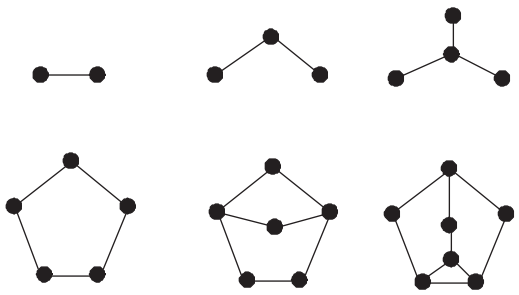


Figure 3.5: Optimal graphs for scenario 3 with $n \in \{2, ..., 7\}$, worst-case information measure.

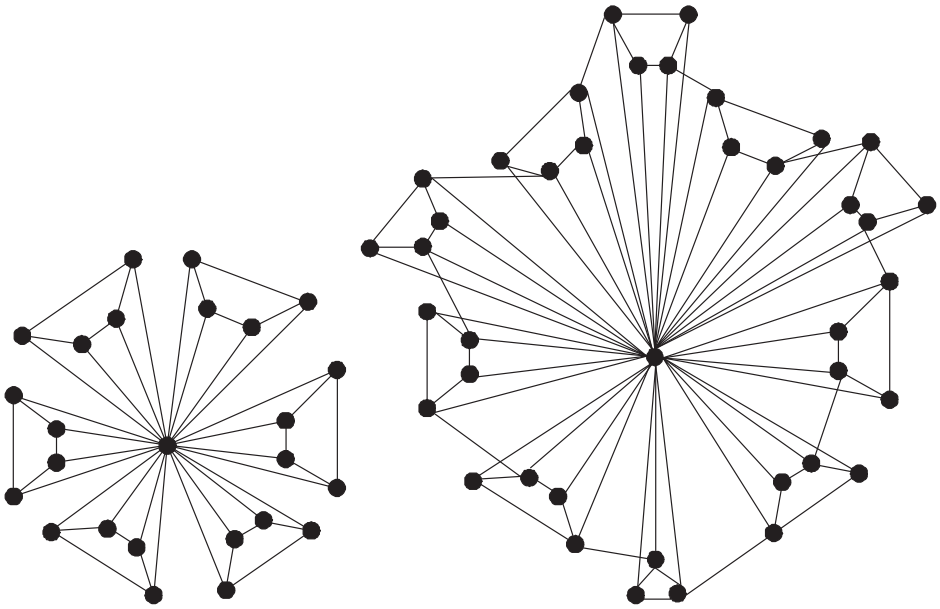


Figure 3.6: Approximate optimal graphs for scenario 3 with n=25 (left) and n=40 (right), worst-case information measure.

(order 25) it can be seen that groups of individuals connected to a central individual appear. The groups correspond to the wings of a windmill, hence we term this structure a *windmill wing graph*. However, if the number of individuals becomes larger (see Figure 3.6 right, order 40 graph) it can be seen that the groups have some connections among each other, therefore we call that structure a *reinforced windmill wing graph*.

3.6 Varying Secrecy and Information Relevance

In Section 3.3 a single optimality criterion was derived by requiring several properties of the solution to the multi-objective optimization problem. By restricting the alternatives to those that satisfy Weak Pareto Optimality, Symmetry, Independence of Irrelevant Alternatives and Covariance with positive scale transformations we arrived at the single bargaining solution, i.e., the graph that maximizes $\mu(g) = S(g)I(g)$. It is possible to extend this analysis by considering organizations that consider a non-balanced tradeoff between secrecy and information. This can be done by dropping the Symmetry requirement. In that case all possible solutions can be parameterized by α such that $\mu(g) = S^{\alpha}(g)I^{1-\alpha}(g)$ is maximized. We provide an initial analysis of network optimality for all three scenarios when varying α, thus explicitly incorporating a criterion that reflects an organization's non-balanced tradeoff between secrecy and informational efficiency. Clearly, the choice of $\alpha = \frac{1}{2}$ corresponds to the analysis as presented in the previous sections.

We present exact results obtained by enumerating all connected graphs of order $n = 7$ for each of the three scenarios presented in Section 3.4 for different values of α. That is, we determine which graph maximizes $\mu(g) = S^{\alpha}(g)I^{1-\alpha}(g)$ given $\alpha = 0.1, 0.2, ..., 0.9$. In addition we present the S, I diagram plotting all S-I combinations for given α, and denote the value of S and I corresponding to the optimal graph by an asterisk. Figure 3.7 shows the $S - I$ diagrams for each value of α in case of scenario 1.

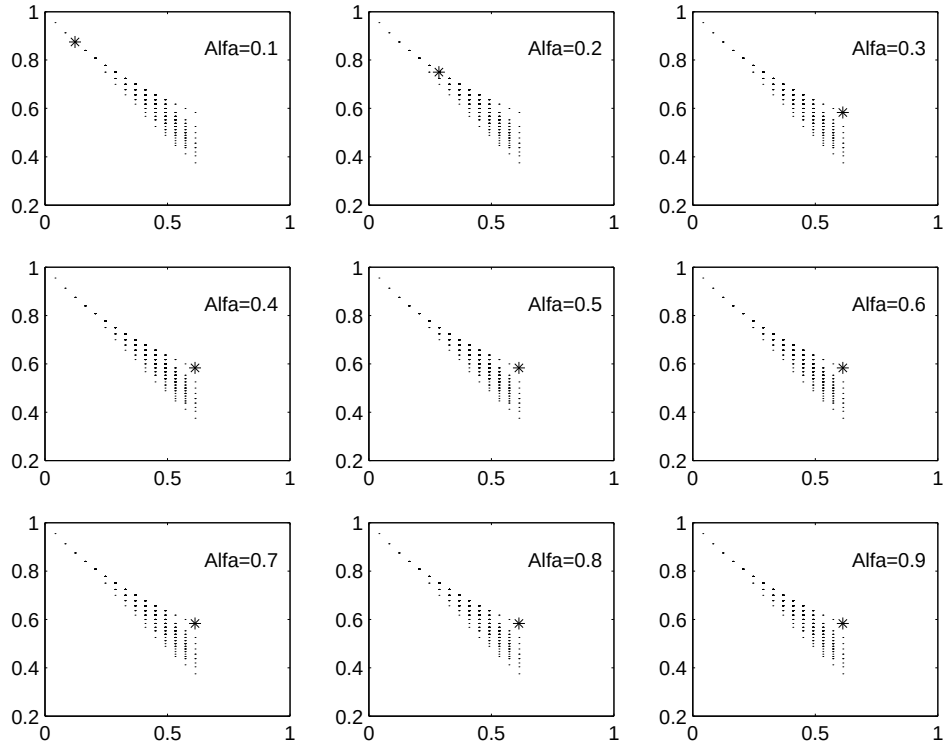


Figure 3.7: Scenario 1: S versus I plots for $\alpha = 0.1$ (top left) to $\alpha = 0.9$ (bottom right), asterisk indicates optimal value.

The graphs that maximize $\mu(g) = S^{\alpha}(g)I^{1-\alpha}(g)$ in case of scenario 1 are shown for each value of α in Figure 3.8.

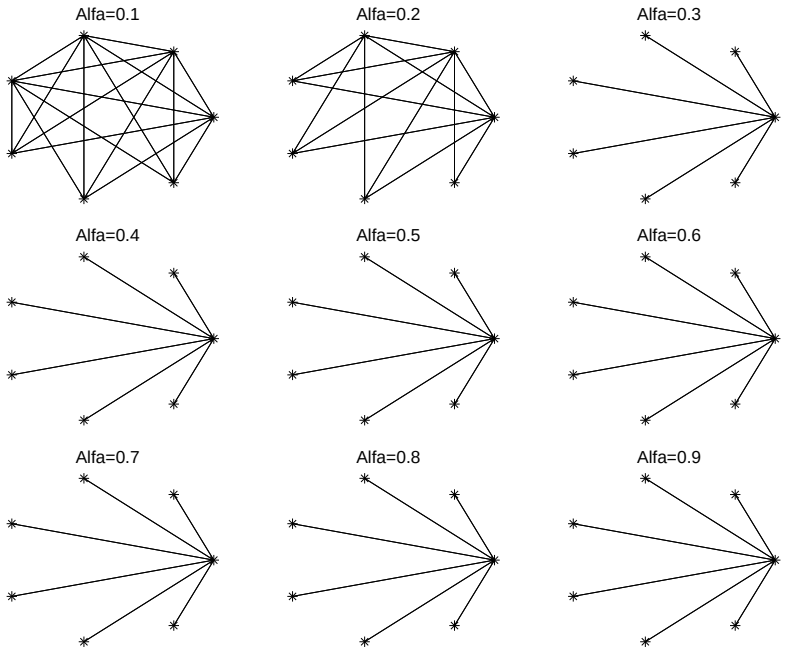


Figure 3.8: Scenario 1: graph that maximizes $\mu = S^{\alpha} I^{\alpha}$ for $\alpha = 0.1$ (top left) to $\alpha = 0.9$ (bottom right).

As expected a covert organization that favors information instead of secrecy will attain a communication structure that is much more dense than an organization interested in secrecy. In addition, the star graph can be seen to be optimal again in case of an organization facing scenario 1 favoring secrecy (high α).

In Figures 3.9 to 3.12 we provide similar plots in case of scenarios 2 and 3.

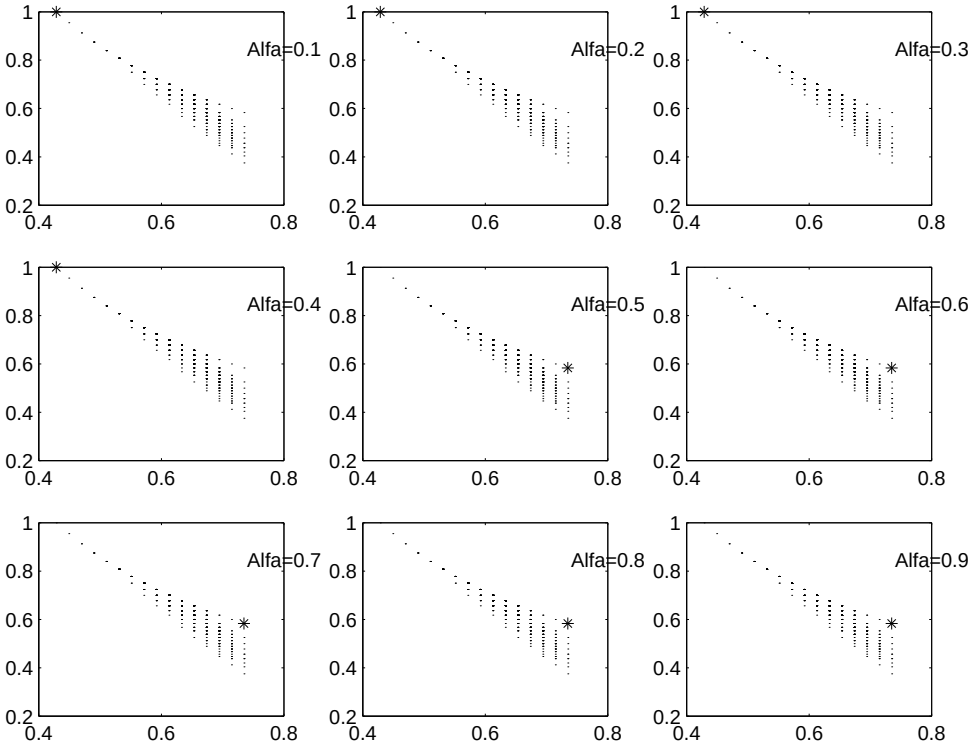


Figure 3.9: Scenario 2: S versus I plots for $\alpha = 0.1$ (top left) to $\alpha = 0.9$ (bottom right), asterisk indicates optimal value.

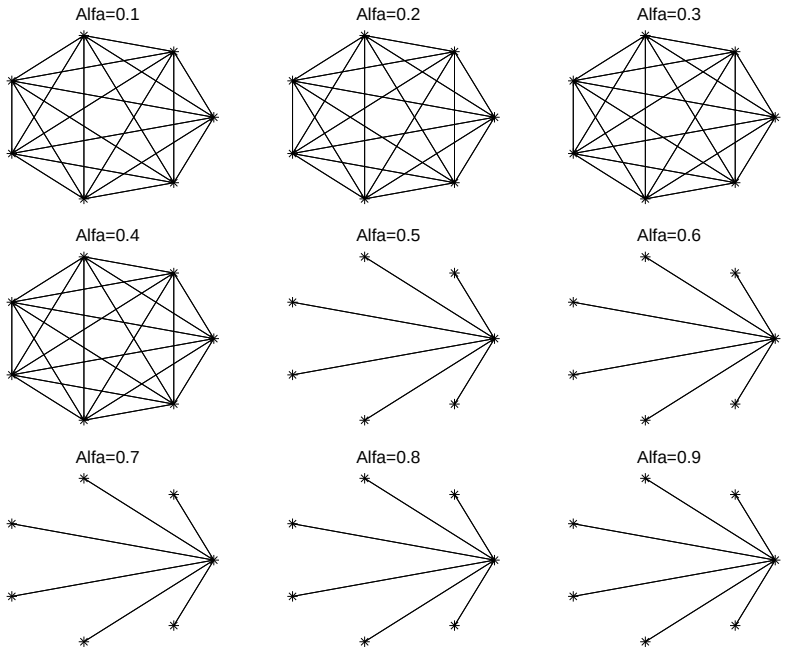


Figure 3.10: Scenario 2, $p = \frac{1}{2}$: graph that maximizes $\mu = S^{\alpha}I^{\alpha}$ for $\alpha = 0.1$ (top left) to $\alpha = 0.9$ (bottom right).

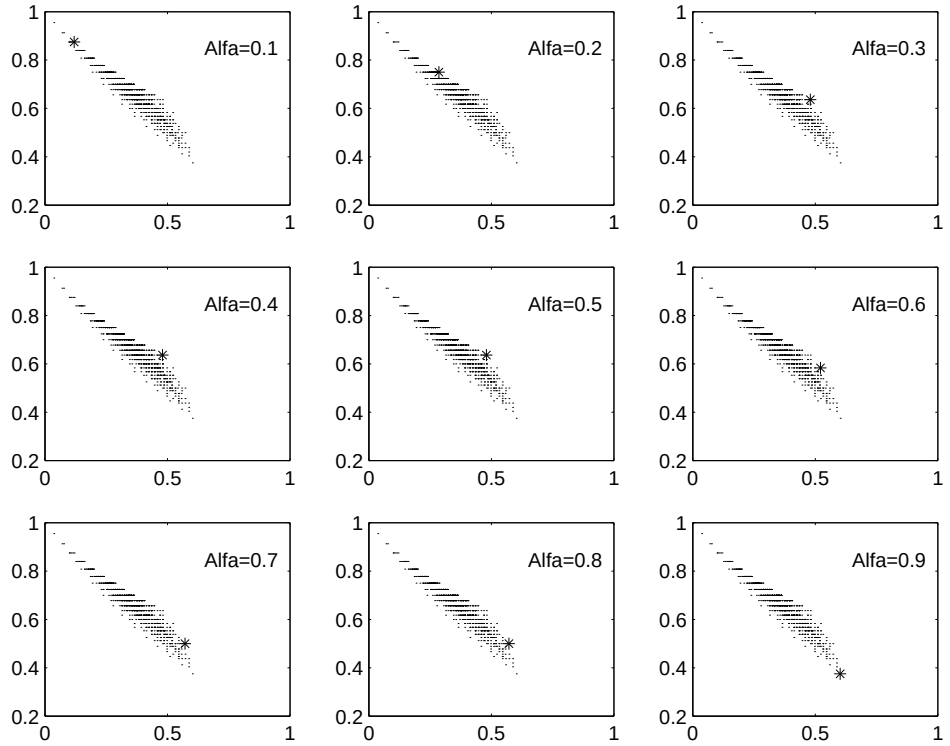


Figure 3.11: Scenario 3: S versus I plots for $\alpha = 0.1$ (top left) to $\alpha = 0.9$ (bottom right), asterisk indicates optimal value.

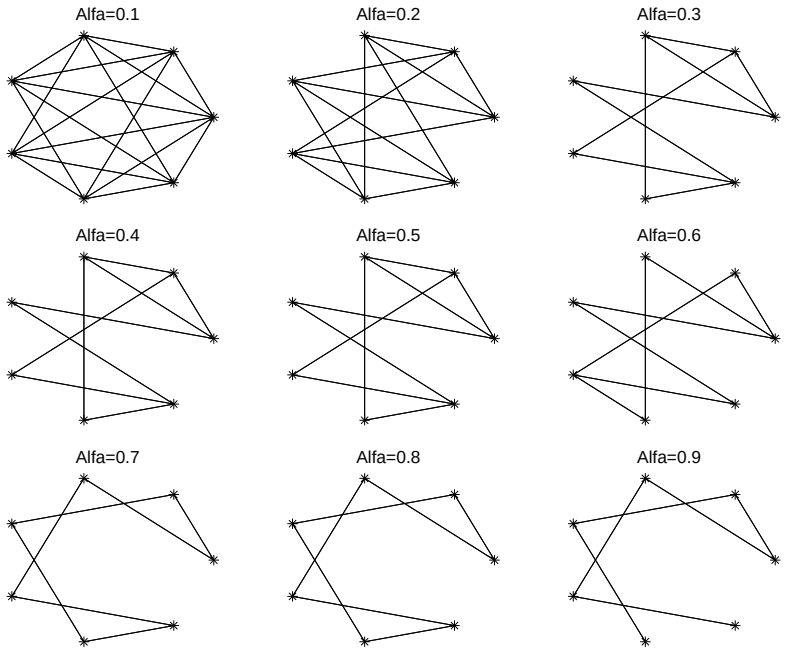


Figure 3.12: Scenario 3: graph that maximizes $\mu = S^{\alpha} I^{\alpha}$ for $\alpha = 0.1$ (top left) to $\alpha = 0.9$ (bottom right).

3.7 Remarks and observations

In this chapter we have analyzed the dilemma every covert organization faces: how to stay secret and at the same time ensure good coordination. We modeled the structure of a covert organization as an undirected graph. The vertices can either be interpreted as individuals in the organization, military units or as terror cells. The selection of the optimal organizational structure was modeled as a multi-objective optimization problem with objectives corresponding to secrecy and operational efficiency of the organization. It was shown that by requiring several properties of the solution a single criterion could be developed to determine the optimal network structure.

Different scenarios were developed and analyzed by assigning a specific information measure and a specific secrecy measure to the set of connected graphs. The first scenario corresponded to a covert organization conducting an operation in its initial stage, in a hostile environment. We established that centralizing information flow by adopting a star network is optimal. The second scenario consisted of a covert organization in its initial stages in an environment of varying hostility. We established that all-to-all communication is optimal in a friendly environment (for instance in a safe-house) and

that the star network is optimal in a hostile environment. The communication structure of a covert network that passed its initial stages in a hostile environment was also analyzed. In the event of such a scenario we established that cellular networks are optimal. Finally a first approach to analyzing covert network communications structures was given by allowing an organization's emphasis on secrecy or information to vary. This resulted in dropping the symmetry requirement and an example of optimal structures in case of order 7 graphs was given.

Our results are consistent with the apparent organizational forms of current terrorist networks, particularly Al Qaeda's 'network of networks'. The results are of twofold use. First they predict the structure of terrorist networks which is important to be able to detect and combat them. Second they aid in the design of military network structures that have to depend on stealth and secrecy. Finally, the analysis in this chapter presents a quantitative theoretical framework for reasoning about covert networks.

There are some avenues for further research. Our model can be extended by generalizing the link detection probability. For instance, the detection probability of a link can be made to depend on properties attached to the vertices of this link. Furthermore, counterterrorism strategies aimed at destabilizing terror networks can be developed and analyzed using the explicit topologies given in this chapter.

Chapter 4

Heterogenous Covert Networks

'Do not go where the path may lead
go instead where there is no path and leave a trail.'
- Ralph Waldo Emerson.

4.1 Introduction

In chapter 3 we discussed a basic framework on covert networks and we made the homogeneity assumption that the ties that exist among individuals are binary, i.e., there either is an interaction or there is not. In reality the nature of interactions between individuals in a covert organization is much more complex.

In this chapter, that is based on Lindelauf et al. [2009b], we present and extend insights into the dilemma of secrecy and operational control in covert networks. To recapitulate, in chapter 3 a secrecy measure and information measure were defined and the Nash bargaining criterion was adopted to determine the optimal covert networks of a given order. Several scenarios were analyzed. First, under the assumption of uniform individual exposure probability and high link detection probability it was shown that a star graph is optimal. However, on the assumption of low link detection probability it was shown that the complete graph is optimal. Second, if the exposure probability of individuals depends on their centrality with regard to information exchange it was shown that cellular networks are optimal. This chapter puts that theoretical framework on homogeneous covert networks to the test by applying it to the 2002 Jemaah Islamiyah Bali bombing and World War II smuggling networks. The theoretical framework does well in explaining most aspects of the network structures that those organizations adopted to carry out their operations. In addition however it is recognized that the nature of interaction between entities in a covert organization is not necessarily homogeneous. Hence the theoretical

framework is extended to incorporate heterogeneity of the network. The most basic heterogeneous network is the network in which all but one of the interactions presents a similar risk to the organization. In Section 4.3 the pair of individuals that should conduct the interaction that presents the highest risk to the organization is the pair that is the least connected to the remainder of the network. In addition, when choosing among a path, star and ring graph with a single high risk interaction pair it is found that for low order graphs the path graph is best. Increasing the order of the network a transition occurs such that the star graph becomes best. It is found that the higher the risk a single interaction presents to the covert network the later this transition from the path to the star graph occurs. Furthermore, approximate optimal networks given a single risky interaction are determined by simulation.

This chapter is organized as follows. The Jemaah Islamiyah 2002 Bali bombing operation and World War II smuggling networks will be discussed in Section 4.2 and compared to the theoretical results on optimal covert networks as presented in chapter 3. In Section 4.3 the theoretical framework is extended to incorporate heterogeneity with respect to the secrecy of interaction between entities in covert networks. Finally in Section 4.4 we analyze the star network structure taking both information and secrecy heterogeneity into account. We will derive the optimal distribution of risk and information exchange over the links of this graph.

4.2 Two empirical examples

In this section we analyze organizations that faced the tradeoff between secrecy and operational efficiency. In doing this we put the theoretical framework of chapter 3 to the test. We analyze how these organizations dealt with this tradeoff by studying and comparing the network structure that they adopted to the theoretical framework.

4.2.1 Jemaah Islamiya Bali bombing

Jemaah Islamiya started as an Indonesian Islamist group and is a loosely structured organization characterized by four territorial divisions (mantiqis) corresponding to peninsular Malaysia and Singapore; Java; Mindanao, Sabah, and Sulawesi; and Australia and Papua [Koschade, 2002]. Abdullah Sungkar, motivated by the need for a new organization that could work to achieve an Islamic State in Indonesia, started JI in Malaysia around 1995. Al Qaeda infiltrated JI during the 1990's and JI subsequently developed into a pan-Asian network extending from Malaysia and Japan in the north to Australia in the south

[Gunaratna, 2003]. By doing this Al Qaeda set out to link these groups into a truly transnational network [Abuza, 2003].

The tactical operation of the Bali attack that was conducted by Jemaah Islamiyah's Indonesian cell is described in Koschade [2006]. We will discuss the importance of certain players in this attack in chapter 7, in this chapter we are interested in the network structure from the perspective of the secrecy versus information trade-off dilemma. The attack was carried out on October 12, 2002, by having a first operative explode a vest of explosives in Paddy's bar. This caused people to flood to the streets, which triggered the second attack by a vehicle born improvised explosive (VBIED) of about 1000 kilograms of TNT and ammonium nitrate. Consequently 202 people were killed. The operational setting consisted of a team of bomb builders located in a safe-house, a separate support team split over two safe-houses and a command team. The individuals in the safe-houses were thoroughly aware of the need for secrecy. This is indicated by the fact that each member used their Balinese alias and that communication occurred in code words. The individuals in the safe-houses rarely left these houses and used methods to reduce the probability of link detection: they only communicated by SMS and they changed their sim cards frequently. Hence, due to the similarity of these individuals from the viewpoint of secrecy, the probability of exposure of the individuals in the safe houses may be assumed to be uniform. In terms of the theoretical framework described in chapter 3 the setting in which these individuals operated reflects the second scenario with low values of p [Lindelauf et al., 2009a]. Hence, the actual subgraph corresponding to these individuals is best compared to the results obtained for this scenario.

To coordinate the operation a command team consisting of five individuals was set up. The operational commanders were highly active with regard to exchange of information. Hence the setting in which the command team members operated fits best to the second scenario with high values of p of the theoretical framework. Hence we compare the actual subgraph corresponding to these individuals to the theoretical results obtained for the second scenario in chapter 3.

Koschade [2006] presents the actual network of this operation as provided in Figure 4.1. It is this graph that we use as a basis for comparison with the theoretical framework presented earlier. We partition the network into three subnetworks corresponding to the groups of individuals with intrinsically different goals. The Bali Bombing cell can be split into the bomb making team (cell 18), the support team (team Lima) and the command team. It can be seen that cell 18 as well as team Lima adopted the structure of a complete

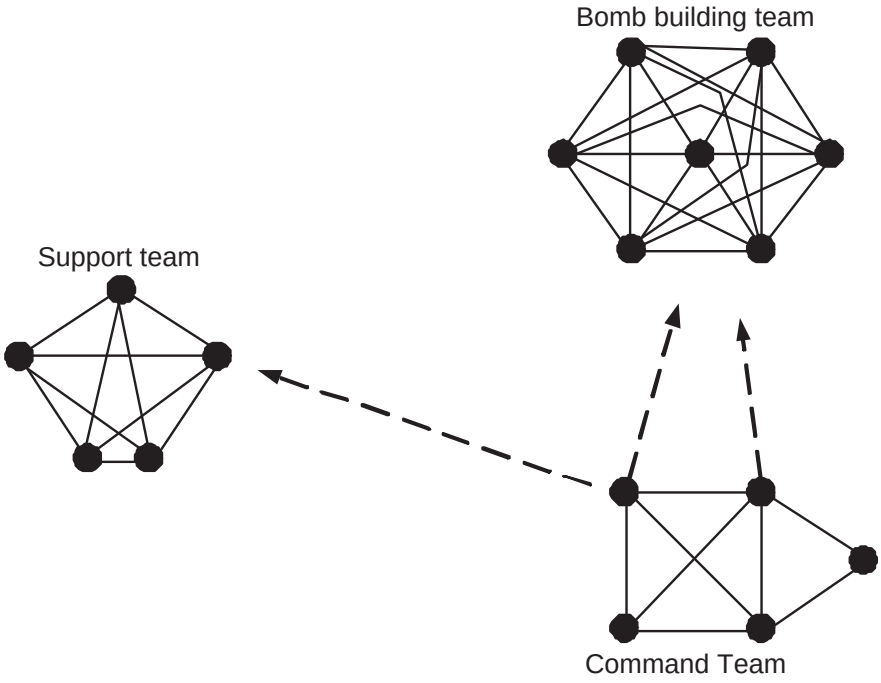


Figure 4.1: Social Network of Jemaah Islamiyah cell that conducted the Bali Operation on October 6, 2002.

graph. That is, by choosing a location with tight security, never leaving the house and having someone on guard they tried to lower the exposure probability and link detection probability as much as possible. Both cells obtained the optimal graph according to the theoretical framework, i.e., they adopted the complete graph which is the optimal graph in case of scenario 2 with low values of p. The command team visited both cells and coordinated the operation.

Figure 4.2: JI Command Team (left) and the theoretically optimal command team (right)

The theoretical framework of Lindelauf et al. [2009a] only considers a homogeneous communication structure, and does not take into account the nature of interaction that this communication represents. In his analysis Koschade considers a weighting function on the edges by scaling the frequency and duration of interaction between 1 and 5.

This already indicates that the nature of interaction among individuals in the network is not homogeneous. The frequency and duration of interaction differed most among the members of the subgraph corresponding to the command team. This non-homogeneity of interactions will be incorporated into the theoretical framework in the next subsection. First however we present another example.

4.2.2 World War II Smuggling Networks

On June 22 1940, France signed an armistice with Hitler Germany causing about 1.5 million French prisoners of war (POW) being detained in German camps. During the war there were multiple breakout attempts as about 71.000 out of 300.000 French POW's managed to escape. The local population actively and passively assisted in the escape of these prisoners of war. Among the regions where the local population assisted was the province of Limburg in the south of the Netherlands. This form of subversive activity often appeared spontaneous, however, the people involved realized that the smuggling routes they facilitated were vulnerable. This because it sometimes occurred that smuggling routes were infiltrated, causing exposure of some of the nodes in the corresponding smuggling network. Therefore the networks were designed such that upon exposure of a node (or upon the arrest of some individuals) other escape routes were available. Hence in the province of Limburg a network of smuggling routes emerged that was designed to efficiently handle the flow of escaping downed aviators and POW's and at the same time ensure the necessary secrecy. For instance, an escapee that more or less randomly appeared at the German-Dutch border would be assisted by a Dutch farmer (who spoke French). This farmer would guide the POW to the local Church where he would obtain further assistance. If an escapee successfully managed to escape to France he would often try to inform his fellow mates still in the prison camp about the route taken. This assisted the spontaneous emergence of these smuggling networks.

It needs no elaboration that the individuals engaged in setting up and continuing the subversive activities to aid the escape of allied prisoners were doing so by improvisation. One can argue that network formation occurred according to the evolutionary dynamics of natural selection: those routes that were not discovered and exposed persisted; those that were infiltrated and exposed perished. The structure of the resulting networks therefore is expected to be a balance of the tradeoff between secrecy and information. Therefore we investigate two of those smuggling routes. Since these smuggling networks operated for an extended period of time, the exposure of a node in the network depended on the

centrality of the respective node in the exchange of POW's. Therefore we will analyze the interior pattern of the smuggling network by comparing the corresponding network structure to the results obtained for scenario 3 in the theoretical framework. That is, we will look at the organization of that part of the network that has to guide the escapees through a certain part of the occupied territory. We will not consider the nodes at which the escapees entered or exited the network because these are typically determined by geographical considerations (such as the existence of waterways and dense forests, etc.). Often the POW's were introduced into the network by local Dutch people that worked in Germany or they arrived at certain villages on their own.

Steyl smuggling route

Starting in 1941 chaplain L.A. Akkermans initiated the creation of a smuggling network to aid the escapees arriving in the region of the towns of Tegelen and Steyl [Cammaert, 1994]. He tried to structure the smuggling of POW's arriving from Germany. Local monasteries functioned as safe-houses. The smuggle route in the region of Tegelen and Steyl consisted of five villages; escapees arrived at Venlo (vn) and were smuggled through Maasbree (ma), Baarlo (ba), Steyl (st) and Belfeld (be) and from thereon routed to Belgium. The theoretical optimal network and the actual network structure are given in the Figures 4.3 and 4.4 below,

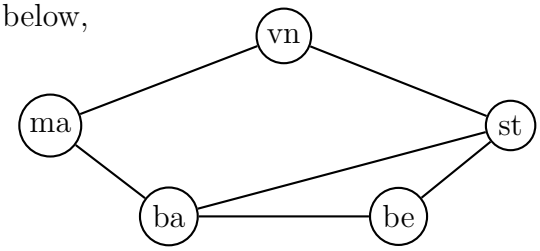


Figure 4.3: The Steyl smuggling route.

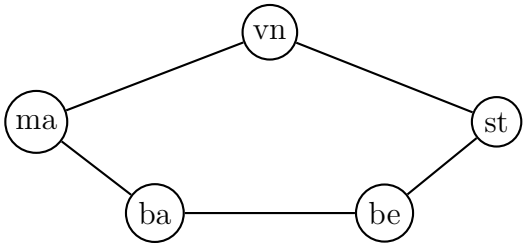


Figure 4.4: Theoretical optimal smuggling route.

It can be seen that the Steyl smuggling network is close to the optimal network. Actually, removing the Steyl-Baarlo route would make it optimal. It is known that the German military conducted regular inspections (randomly) but they never disclosed any

actual POW being smuggled. The Germans suspected smuggling to be taking place (they arrested at least five people in the region) but were never able to expose the network. It is assumed that about 150 to 250 people were smuggled throughout this region.

Maasbree and Baarlo smuggling route

Several other smuggling routes West of the river Maas comprised of the nine villages Grubbenvorst (gr), Velden (ve), Venlo (vn), Tegelen (te), Steyl (st), Belfeld (be), Baarlo (ba), Maasbree (ma) and Sevenum (se). Again chaplain Akkermans from Tegelen contributed to this network. Because of the close proximity of Baarlo to the river Maas a lot of pow's coming from Steyl crossed this town. The actual (Figure 4.5) and an approximated optimal (Figure 4.6) network structure are shown below.

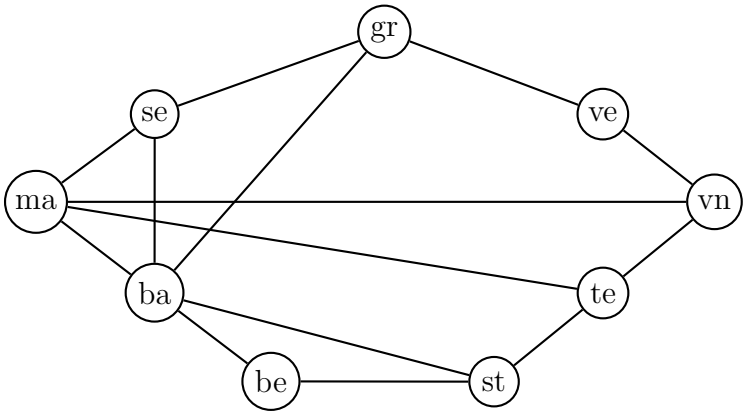


Figure 4.5: The Maasbree and Baarlo smuggling route.

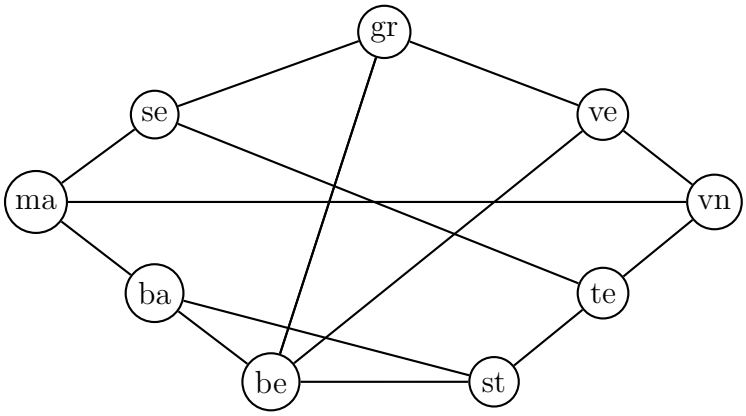


Figure 4.6: The approximate theoretical optimal smuggling route.

The optimal networks in chapter 3 are unlabeled, i.e., there are multiple ways in which such an optimal network can be 'fitted' on labeled vertices. Even so, one can wonder how 'close to the optimal network' the network in Figure 4.5 actually is. The optimal configuration can be obtained by the 'actual' one only by changing 3 routes: Tegelen-Maasbree to Tegelen-Sevenum, Grubbenvorst- Baarlo to Grubbenvorst - Belfeld and changing Sevenum-Baarlo to Velden-Belfeld.

One caveat is that optimality in both our cases only considers the network structure, i.e., changing the node labels without altering the network structure does not change the degree of optimality of the corresponding network. Hence there are multiple distinct labeled networks that can be obtained by changing only a few links with respect to the optimal ones. This should be taken into account when discussing the relative optimality of a network.

4.3 Secrecy Heterogeneity

As is clear from the previous two examples, an organization conducting a covert operation not only has to consider the structure of its network but also has to take into account that the nature of interaction between the nodes is not homogeneous. For instance, the act of delivering a pre-manufactured bomb to the triggerman in an IED network is potentially more dangerous than the internal communication (possibly through codewords) discussing the planning of an attack. Therefore we will extend the theoretical framework on covert networks by differentiating between the nature of interaction among individuals. Two questions come to mind. First, given a network structure, which pair of individuals should conduct the interaction that presents the highest risk to the organization? Second, given the fact that there is a pair of individuals conducting an interaction that presents a high risk to the organization which network structure is optimal?

4.3.1 The Optimal High Risk Interaction Pair

We consider the situation that the interaction between individuals in the network is not completely homogeneous. This occurs among others because the frequency, duration and nature of interaction differs between individuals. Hence, certain interactions present a higher risk to the organization than others. We model this by assigning 'weights' to the links, representing the risk of that interaction. For graph $g = (N, E)$ we define the weighting function $w : E \to [1, \infty)$ such that $w_{ij} > w_{kl}$, $ij, kl \in E$, is interpreted as interaction between individual i and j presenting a higher risk to the organization

than interaction between k and l. Denote the set of all such weighting functions by $\mathbb{W}$. Explicitly we denote a graph g with weight $w \in \mathbb{W}$ assigned to its edges by $g(w)$. The interpretation of this weighting function forces us to adjust the definition of secrecy. The information measure needs not to be adapted: one either interacts with an individual or not. However, risky interactions provide an enhanced security threat to the organization.

We adjust the secrecy measure corresponding to the first scenario in chapter 3. For $g \in \mathbb{G}(n,m)$ we set $u_i = 1 - \frac{d_i(g)+1}{n}$ but adjust the probability of detection of an individual. This probability of detection now not only depends on *the number* of individuals this individual is connected to but also on the nature of that interaction.

Let

$$w_i = \sum_{j \in \Gamma_i(g)} w_{ij}$$

where $\Gamma_i(g) = \{j \in N | ij \in E\}$ and define,

$$W(g) = \sum_{i \in N} w_i = 2 \sum_{ij \in E} w_{ij}. \tag{4.1}$$

Motivated by the fact that a risky interaction increases the relative probability of exposure of an individual we set $\alpha_i = \frac{w_i+1}{W(g)+n}$. In case $w_{ij} = 1$ for all $ij \in E$, α_i reduces to π_i as given in Section 3.4.3, i.e., $\alpha_i = \frac{d_i(g)+1}{2m+n}$. Secrecy is again defined by

$$S(g) = \sum_{i \in N} \alpha_i u_i.$$

It can be seen that the secrecy measure of a graph g is the expected fraction of the network that survives upon exposure of an individual in the network according to probability distribution $(\alpha_i)_{i \in N}$. It is easily derived that

$$S(g) = \frac{n^2 - 2m - n + W(g)(n-1) - \sum_{i \in N} d_i(g) w_i}{n(W(g)+n)}. \tag{4.2}$$

It follows that $S(g^n_{comp}) = 0$. Slightly more general for any k-regular graph $g \in \mathbb{G}^n$ it holds that $S(g) = 1 - \frac{k+1}{n}$.

With $I(g) = \frac{n(n-1)}{T(g)}$ we find that,

$$\mu(g) = S(g)I(g) = \frac{(n-1)}{T(g)} \frac{n^2 - n - 2m + W(g)(n-1) - \sum_{i \in N} d_i(g) w_i}{W(g)+n}. \tag{4.3}$$

The following result is readily obtained,

Lemma 4.3.1

(i) $\mu(g^n_{star}) = \frac{n-2}{2n-2} \cdot \frac{n-1+\frac{1}{2}W(g^n_{star})}{n+W(g^n_{star})}$.

(ii) $\mu(g^n_{path}) = \frac{3}{n+1} \cdot \frac{(n-2)(n-1)+(2n-6)W(g^n_{path})+w_{12}+w_{n-1,n}}{n(W(g^n_{path})+n)}$ *if the path is given by 1,2,...,n-1,n.*

(iii) $\mu(g^n_{ring}) = \begin{cases} \frac{4n-12}{n(n+1)} & \text{if } n \text{ is odd} \\ \frac{4(n-3)(n-1)}{n^3} & \text{if } n \text{ is even} \end{cases}$

Due to the symmetry of g_{ring} and g_{star} the interaction that presents the highest risk can be conducted by any pair of individuals. This can also be seen directly from Lemma 4.3.1.

In addition we determine the optimal location of the highest risk interaction for the path graph. The best position (in terms of maximizing μ) in the path graph is between either pair of individuals such that one of these individuals is an endpoint of the path. So, if the path is given by $1, 2, ..., n-1, n$ then w_{12} or w_{n-1n} is maximal. Thus an organization structured as a path graph does best by having either pair of players conducting the risky interaction as far away as possible from the central players. This is in accordance with intuition.

In general it is shown that the pair of individuals in the organization that should conduct the interaction that presents the highest risk to the organization is the pair that is the least connected to the remainder of the network.

Theorem 4.3.1 *Let* $g = (N, E) \in \mathbb{G}(n, m)$ *and* $\{kl\} = argmin_{ij \in E}\ (d_i + d_j)$. *Set* $\hat{w}_{kl} = W - (m-1)$, $\hat{w}_{ij} = 1$ *for all* $ij \in E \setminus \{kl\}$. *Then* $\mu(g(\hat{w})) > \mu(g(w))$ *for all* $w \in \mathbb{W}$ *with* $\sum_{ij \in E} w_{ij} = W$.

Proof:
It can be seen from equation 3.3 that, given a graph $g \in \mathbb{G}(n, m)$ and total weight $W = \sum_{ij \in E} w_{ij}$, maximizing $\mu(g)$ is equal to minimizing $\sum_{i \in N} d_i w_i$. It readily follows that $\sum_{i \in N} d_i w_i = \sum_{ij \in E} w_{ij}(d_i + d_j)$. Hence the result follows. □

Given the situation that only a single interaction presents a higher risk to the organization we now compare the optimal path, star and ring graph using these results. We analyze the situation of a slightly riskier interaction ($z = 2$) and the situation of a much more riskier ($z = 100$) interaction. Clearly the graphs are chosen such that the high risk

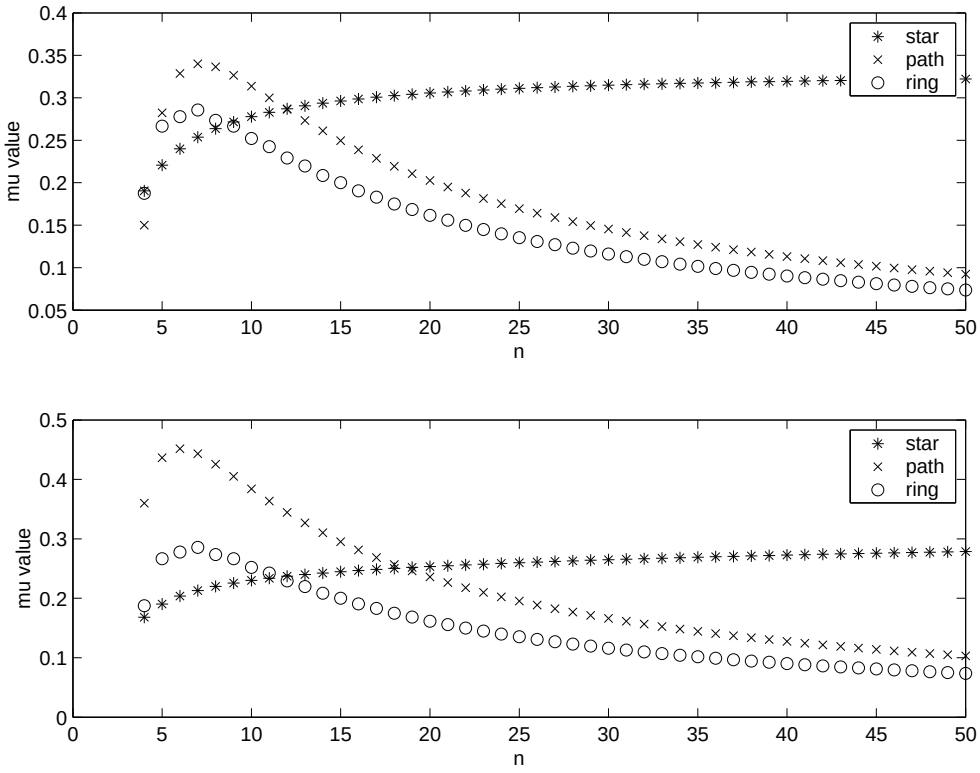


Figure 4.7: A comparison between star, path and ring graph for z=2 (top) and z=100 (bottom).

interaction is conducted on a link in the respective graphs. The results are summarized in Figure 4.7. The ring graph is always dominated. It can be seen that for low values of n the path has a higher value of μ than the star graph. At a certain value of n a transition occurs such that $\mu(g^n_{path})$ becomes smaller than $\mu(g^n_{star})$. In case of $z = 2$ this transition occurs at $n = 11$. In case $z = 100$ this transition occurs at $n = 18$. Thus it can be seen that the amount of risk an interaction poses to the organization influences this transition point. For instance imagine one has to consider an organizational form that either is very centralized (star graph) or decentralized (path graph). If the number of individuals in the organization, i.e., n, is very large the star graph is the better choice. This can be understood intuitively because of the difficulty of information exchange in large path graphs as opposed to star graphs. However, if there is a single interaction that is much more risky relative to the others it still is advantageous to adopt a path graph organizational form. Clearly, this reduces the capability to process information but from the perspective of secrecy has the advantage of reducing the risk to the organization by positioning the risky interaction as far away as possible from the central players.

4.3.2 Approximating Optimal Secrecy in Heterogeneous Covert Networks

In Section 4.3.1 it was established that if there exists exactly one pair of individuals that conduct an interaction that presents a high risk to the organization they should have the least connection to the remainder of the network (theorem 4.3.1). In this section we are interested in *which* connected graph $g \in \mathbb{G}^n$ should be adopted given the fact that the pair of individuals $i, j \in N$ conducting the risky interaction is the one that minimizes $d_i + d_j$. We approximate the graphs that are optimal in this respect by simulation.

We conducted a greedy optimization algorithm as follows.

Algorithm for approximating optimal single risk interaction network.
Input:
Initial graph: $g^n_{initial}$.
Value of risky interaction: z.
Number of times edges are added: m.
Initialization:
$\bar{g} = g_{initial}$. (Denote $\bar{g} = (N, E)$).
$\mu(g_{help}) = 0$.

Iteration 1:
For i = 1:m

Iteration 2:
For $kl \in E^c$
Step 1. Set $g' = \bar{g} \cup kl$.
Step 2. Determine $i, j \in g'$ such that $d_i + d_j$ is minimal and locate z at this link.
Step 3. Compute $\mu(g')$.
Step 4. If $\mu(g') > \mu(g_{help})$ set $g_{help} = g'$.

End iteration 2.
$\bar{g} = g_{help}$.

End iteration 1.
Output:
$\bar{g}$.
$\mu(\bar{g})$.

The best results, which depend on the initial graph, of this greedy optimization are presented in Table 4.1 for graphs of order $4 \leq n \leq 10$. The location of the pair of individuals that conduct the interaction that presents a high risk to the organization is presented in bold.

4.4 Secrecy and Information Heterogeneity

Hezbollah's organizational structure during the 2006 IDF war in southern Lebanon is another example of the ability to successfully adopt and exploit network centric warfare concepts by a non-state actor. Hezbollah acted as an informal and adaptive distributed network of small cells and units that were acting with considerable independence and were capable of rapidly adapting to the local conditions [Cordesman et al., 2007]. In the previous sections we not only investigated such communication structures, but also the influence of varying degrees of risk interactions present to the organization. This resulted in a first approach to heterogeneity in covert networks. It was assumed that high risk interactions affect the exposure probability of individuals in the organization (and hence the secrecy measure), not the amount of information that potentially could be exchanged. For instance consider the delivery of bomb making materials between individuals of the

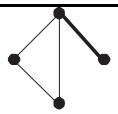
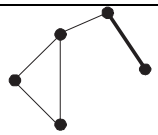
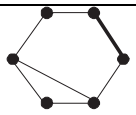
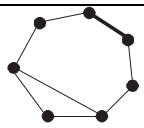
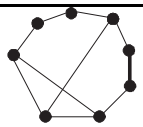
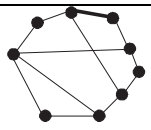
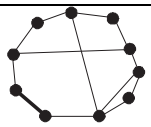
n	initial	final	μ
4	path		0.2813
5	path		0.2837
6	ring		0.3021
7	ring		0.3010
8	ring		0.3062
9	ring		0.3141
10	ring		0.3129

Table 4.1: Approximate optimal graphs with single high risk interaction, $z = 2$, indicated in **bold**.

organization. This interaction presents a higher risk to the organization than individuals discussing target sites. However, it bears no influence upon the amount of information exchange inside the organization: there either is such a risky interaction or there is not. Therefore the information measure in Section 4.3 was not adapted.

The focus of this section is on secrecy *and* information heterogeneity, because there might also be situations where both can be considered to be not homogeneous. As a first approach we analyze star networks. This prototype network can for instance represent an arms smuggling network where the center of the network corresponds to the agency distributing the arms between its various outposts. Note that the real world exhibits many (non-covert) networks shaped as stars. Consider for instance a hub and spoke network of air-carriers or sensor networks where there is one base station and several

sensors communicating with it. Thus the study and analysis of such star networks could also yield results directly applicable to non-covert network problems. In addition there are covert networks adopting star topologies: an actual covert network that adopted the star network structure, discussed in chapter 3, is that of the Dutch National Clandestine Service's so-called 'stay behind organization'. In this section we will investigate the optimal distribution of risk and information exchange in such a star network.

4.4.1 Star Networks

Motivated by the fact that in the baseline scenario as described in Section 3.4.1 the star network is optimal we further analyze the star network topology. This section is based on Lindelauf et al. [2008]. We assume that not only is it possible to have interactions that are heterogeneous with respect to secrecy but also that there are interactions that provide an opportunity in varying the amount of information exchange. We analyze the optimal distribution of this risk and information exchange over the star network topology.

Example 4.1:
Consider an arms smuggling organization consisting of five regional outposts and a central distributing agency in the form of a star graph, see Figure 4.8. The central distributing agency is denoted by 'C' and the outposts are indexed 'K' through 'O'. If the situation is such that the exposure probability of each vertex is equal, for instance if the organization is located deep in a jungle and military incursions are rare, and secrecy and information are considered homogeneous, Lindelauf et al. [2009a] showed that the star structure is optimal. However, now consider the same organization in a transnational setting. Additionally assume that the exchange of weapons between the distributing agency and its outposts may vary. Thus looking at Figure 4.8 (Right) twice as much weapons are smuggled on link CM as compared to link CL. Similarly, three times as much weapons are smuggled on link CO with respect to link CL, etc. It can be argued that the risk of smuggling weapons between the agency and an outpost depends linearly on the amount of goods smuggled. In addition, the more material that can be exchanged the better the performance of the organization, from a smuggler's perspective. Thus we assume that the numbers corresponding to the links in Figure 4.8 (Right) 'represent' the risk and information exchange. ◇

We define a function to represent the *risk* an interaction presents by $t : E \to [1, \delta_S]$. Here δ_S is the maximum value a risky interaction can attain (S: secrecy). In the context of smuggling this could be representative of the fact that there is a maximum smuggling

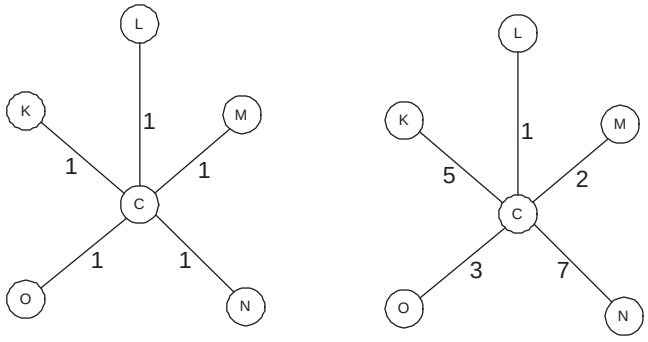


Figure 4.8: Homogeneous star (Left) and heterogeneous star (Right).

capacity. Another function, $c : E \to [1, \delta_I]$ is defined to represent the amount of information exchange between the respective vertices, with similar considerations on δ_I (I: information). In addition of course $c_{ij} > c_{kl}$ with $ij, kl \in E$ implies that the amount of information exchanged between individuals (terror cells, military units, human traffickers) i and j is higher than the amount of information exchanged between individuals k and l (similar considerations hold for the risk function). We denote the graph $g = (N, E)$ with risk weighting function t and information weighting function c explicitly by $g(t, c)$. Note that 'information exchange' depends on the context under consideration. For instance, in the context of human trafficking an interaction represents humans being smuggled: i.e., in that context a higher amount of information exchange corresponds to more humans being trafficked.

The function representing the risk of an interaction and the function representing the amount of information exchange need not be equal in general. An interaction may be risky but not provide any possibility in increasing the amount of information to be exchanged. However, there are types of interactions such that the more information is exchanged the riskier the interaction becomes. It may be argued that this is the case for human trafficking for instance. The interaction between entities in the trafficking network consists of exchanging people. The more people that are exchanged over a link in the network the 'better', preferably yielding a higher information measure. However, the possibility of detection also becomes higher, hence the influence on secrecy. In this situation it can be argued that $t = c$, or at least that there is some positive linear relation between the two functions.

We now define the information measure $I(g(t, c))$. Intuitively the optimal graph in the sense of heterogeneous information exchange is the complete graph $g_{comp}(t, c)$ with

maximum weight on all its edges. First we define *resistances* on the edges. The resistance of edge $ij \in E$ is defined to be the reciprocal of the measure for information exchange, i.e., $r_{ij} = \frac{1}{c_{ij}}$. Denote a path between vertex i and j in graph g by $P_{ij}(g)$. The 'distance' between vertex i and j is defined as the shortest *resistance-weighted* path between i and j:

$$l_{ij}(g(t,c)) = min_{P_{ij}(g(t,c))} \sum_{kl \in P_{ij}(g(t,c))} r_{kl}.$$

The associated total distance is $T(g(t,c)) = \sum_{i,j \in N \times N} l_{ij}(g(t,c))$. The information measure of graph $g(t,c)$ is defined by,

$$I(g(t,c)) = \frac{\frac{1}{\delta_I} n(n-1)}{T(g(t,c))}. \tag{4.4}$$

The function $c : E \to [1, \delta_I]$ that assigns the maximum weight to all edges of graph $g = (N, E)$, i.e, $c_{ij} = \delta_I$ for all $ij \in E$, is denoted by $\bar{c}$. Since $T(g^n_{comp}(t, \bar{c})) = \sum_{i,j \in N \times N} l_{ij}(g^n_{comp}(t, \bar{c}) = n(n-1)\frac{1}{\delta_I}$, the complete graph with maximum weight w.r.t. information at all its edges attains the highest information measure, in accordance with intuition, i.e., $I(g^n_{comp}(t, \bar{c})) = 1$.

The total risk individual i is engaged in is defined by $t_i = \sum_{j \in \Gamma_i(g)} t_{ij}$, where $\Gamma_i(g) = \{j \in N | ij \in E\}$. The heterogeneous secrecy measure (equation 4.2) with risk function t and total weight $W_t = \sum_{i \in N} t_i = 2 \sum_{ij \in E} t_{ij}$ becomes

$$S(g(t,c)) = \frac{n^2 - 2m - n + W_t(n-1) - \sum_{i \in N} d_i t_i}{n(W_t + n)}. \tag{4.5}$$

The value of W_t can be interpreted as the total risk the organization is engaged in. Given a value for W_t the question then becomes how to optimally distribute this total risk among its edges.

In chapter 3 it was argued that a good criterion for optimality of a graph g is the Nash bargaining value, i.e., the graph g that maximizes $\mu(g) = S(g)I(g)$. For graph $g(t,c)$ this value is given by

$$\mu(g(t,c)) = \frac{n-1}{\delta_I T(g(t,c))} \cdot \frac{n^2 - 2m - n + W_t(n-1) - \sum_{i \in N} d_i t_i}{(W_t + n)}.$$

We analyze the star graph with equal weighting functions corresponding to secrecy and information interactions, i.e, with $t = c$. Thus we assume that the interaction is of such a type that if the information exchange it presents increases the risk increases accordingly. In case of arms smuggling this relation seems a good first approximation.

In fact, in case of a star graph organizational design,with the nature of interactions such that the risk and information weighting functions are equal, it follows that optimally a given total amount of information exchange (and hence risk) should be distributed equally among the links:

Proposition 4.4.1 *Let* $g = g^n_{star}$ *and* $\hat{t} = (\frac{\frac{1}{2}W}{n-1}, \frac{\frac{1}{2}W}{n-1}, ..., \frac{\frac{1}{2}W}{n-1})$. *Then*

$$\mu(g(\hat{t}, \hat{t})) \geq \mu(g(t,t)) \quad \textit{for all } t \in [1, \delta_I]^{n-1}.$$

Proof:
It readily follows that $\sum_{i \in N} d_i(g)t_i(g) = \frac{1}{2}nW$. In addition it can be seen that

$$T(g) = 2(n-1)\sum_{kl \in E} \frac{1}{t_{kl}},$$

such that

$$\mu(g) = \frac{n^2 - 3n + 2 + W(\frac{1}{2}n - 1)}{2\delta_I(W+n)\sum_{kl \in E} \frac{1}{t_{kl}}}.$$

Hence, given the constraint that

$$\sum_{i \in N} t_i = 2\sum_{ij \in E} t_{ij} = W,$$

$\mu(g(t,t))$ is maximized if $\sum_{kl \in E} \frac{1}{t_{kl}}$ is minimized.

Denote the number of elements t_{kl} of $t \in [1, \delta_I]^m$ such that $t_{kl} = \frac{\frac{1}{2}W}{m}$ with $k(t)$ (clearly $k(t) \leq m$) and let $f(t) = \sum_{ij \in E} \frac{1}{t_{ij}}$. Take $\hat{t} \in [1, \delta_I]^m$ such that $k(\hat{t}) < m$. We will construct a $\hat{t}'$ such that $f(\hat{t}') < f(\hat{t})$ while $k(\hat{t}') > k(\hat{t})$. Iterating this procedure yields the result.

Now consider $\hat{t}_{ab}$ and $\hat{t}_{cd}$ such that $\hat{t}_{ab} < \frac{1}{2m}W$ and $\hat{t}_{cd} > \frac{1}{2m}W$. Assume $\frac{1}{2m}W - \hat{t}_{ab} < \hat{t}_{cd} - \frac{1}{2m}W$ (the other case can be dealt with similarly). We set $\hat{t}'_{ab} = \frac{1}{2m}W$ and $\hat{t}'_{cd} = \hat{t}_{cd} - (\frac{1}{2m}W - \hat{t}_{ab})$. This mapping clearly has a unique fixed point: $(\frac{\frac{1}{2}W}{m}, \frac{\frac{1}{2}W}{m}, ..., \frac{\frac{1}{2}W}{m})$. It also readily follows that

$$f(\hat{t}') = f(\hat{t}) - (\frac{1}{\hat{t}_{cd}} + \frac{1}{\hat{t}_{ab}}) + \frac{1}{\frac{1}{2m}W} + \frac{1}{\hat{t}_{cd} - \frac{1}{2m}W + \hat{t}_{ab}}.$$

Easy calculus yields

$$(\frac{1}{\hat{t}_{cd}} + \frac{1}{\hat{t}_{ab}}) > \frac{1}{\frac{1}{2m}W} + \frac{1}{\hat{t}_{cd} - \frac{1}{2m}W + \hat{t}_{ab}}$$

and hence $f(\hat{t}') < f(\hat{t})$. □

Consider the example of arms trafficking again. It was argued that in this case the information and risk weighting functions can be considered equal. If such an organization adopts a star graph design, i.e., a central 'distributing agency' distributing weapons from one place to another, they would perform best by distributing the number of weapons (shipments) evenly across each link. See Figure 4.10 below.

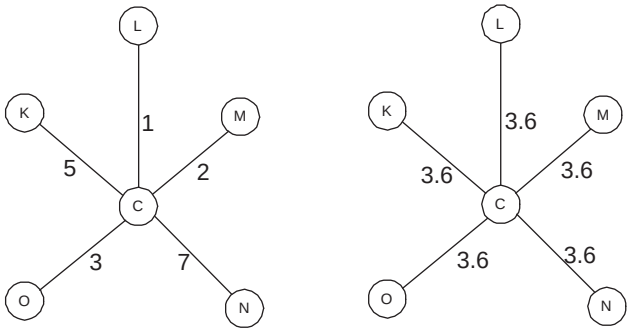


Figure 4.9: A star network with total risk of 18 (Left and Right), optimally distributed (Right).

4.5 Remarks and Observations

In this chapter we relaxed the homogeneity assumption that we made in chapter 3 on the basic covert network model. We motivated this relaxation by use of two empirical examples, Jemaah Islamiyah's Bali attack and WW-II smuggling networks. In Section 4.3 we showed how risky interactions can be modeled by introducing weights on the links and showed that the pair of individuals in the covert organization that should conduct the interaction that presents the highest risk to the organization should be the least connected pair. Additionally we analyzed and presented (approximate) optimal secrecy heterogenous networks. Finally we analyzed both secrecy and information heterogeneity in case of star networks and concluded that optimally a given total amount of information exchange should be distributed equally among the links.

Chapter 5

Covert Affiliation Networks

'Better to fight for something than live for nothing.'
- George S. Patton

5.1 Introduction

Some attention has already been given to the use of OR/MS tools and experiments in the domain of anti-terrorism planning, for instance in how to best respond to an anthrax attack [Craft et al., 2005] or on using queuing theory to analyze scheduling policies in a surveillance system to detect terrorists in time [Lin et al., 2009]. Other examples include studies into the costs and disruptions that might arise if U.S. domestic airlines adopted an antiterrorist measure aimed at preventing baggage unaccompanied by passengers from traveling in aircraft luggage compartments [Barnett, 2001] and models that identify resource-limited interdiction actions that maximally delay the completion time of a nuclear's weapons project [Brown et al., 2009]. What is clear from the current war on terror is that many decision makers in law enforcement, the military and other security organs face opponents of a nature quite different than they were used to: asymmetrical, irregularly operating groups and organizations. In this chapter we present a model of covert *affiliation* networks that can function as a guide and benchmark of hybrid organizations.

Traditional models of organizations do not fully apply to organizations such as Al Qaeda which is said to have transformed from a hierarchical terrorist organization to a multifaceted 'network of networks'[Tucker, 2001]. Similarly Hamas abandoned its centralized, leadership structure and developed a compartmented organizational structure of sparsely overlapping cells [Gambill, 2002]. More generally many covert organizations

today, be they criminal, terrorist or insurgent, have profited from the shift to networked organizational forms [Arquilla and Ronfeldt, 2001], [Asal et al., 2007]. These covert organizations assign tasks to cells to complete an operation. Furthermore there is coordination and control among these cells to ensure operational success. Even in case of autonomous cell formation those cells need to be directed, i.e., they need strategic guidance [Cruickshank and Hage Ali, 2007]. This covert organizational form has been studied mostly from a qualitative perspective [Asal et al., 2007], [Mishal and Rosenthal, 2005]. Since it is important to develop a more general framework in which the structure of a covert network can be predicted and analyzed several formal models have been developed [McAllister, 2004], [McCormick and Owen, 2000], [Enders and Su, 2007]. What is recognized in this regard is the fact that the requirement for secrecy distinguishes the covert organization from the overt organization [Baker and Faulkner, 1993]. Taking this dilemma explicitly into account we analyzed the problem of covert network structure design from a multi objective optimization perspective in chapters 3 and 4. In this chapter we build upon this research by extending the analysis to the case of covert *affiliation* networks. What we adopt from chapter 3 is the method of measuring secrecy and information in networks. However we do not restrict ourselves to 'simple' networks, instead fundamentally different and new is the restriction to the domain of covert cells modeled by affiliation networks. We focus on affiliation in cells because covert organizations employ cells consisting of several individuals needed to complete a task. Furthermore, these cells have to be coordinated and controlled to better guarantee mission success. Common types of such cells are for instance a command and control cell, a tactical operations cell, an intelligence cell and a logistics cell [Nance, 2008].

In sociology the term *affiliation* is used to refer to data on the participation of actors in events. Common examples include corporate board memberships [Mizruchi and Bunting, 1981, 1983; Mizruchi, 1994], [Lester and Cannella, 2006] or participation in online groups [Allatta, 2003, 2005]. Much research on empirical and theoretical aspects of affiliation networks has been conducted. It is not difficult to imagine affiliation relations within the domain of covert networks. What is clear is that terrorist, insurgent and criminal organizations use networked organizational forms to remain secret while ensuring mission success, i.e., they exchange information in communication networks, smuggle weapons through trafficking networks and their councils meet in affiliation networks. Hence these actors and their actions can also be viewed from the perspective of affiliations, i.e., the binary relationships consist of relationships between covert organizational members and their participation in cells.

Overt affiliation networks have been studied abundantly. Examples include interlocking boards of directors [Levine, 1972], [Mariotti, 1998], [Mintz and Schwartz, 1981], [Allen, 1982], [Bearden and Mintz, 1987], club memberships [Bonacich, 1978] and social gatherings [Breiger, 2004]. However very few, if any, *affiliation* network analysis has been done in the important domain of covert networks taking the aspect of secrecy explicitly into account. In this chapter, based on Lindelauf et al. [2010] we will present a general framework to analyze covert cells by evaluating them on the basis of the one-mode projection of the corresponding affiliation network.

Analyzing cell structured affiliation topologies is of twofold importance: it increases the understanding of their structure and henceforth helps to improve strategies to counter them, and it enables military organizations to optimize their covert operations. Perhaps the best known example of a covert operation conducted according to cell structured affiliations is provided by Al Qaeda's 9/11 operation. The organizational structure of the covert group conducting that operation equalled 4 cells of 19 people [Zwikael, 2007]. Additionally there was a command and control 'cell' guiding the operation, consisting of Khalid Sheikh Mohammed, Mohammed Atef and Osama Bin Laden. A more historical, nation-state, example is the case of Israeli's operation Susannah [Johnson, 2007], [Golan, 1978]. The belief among Israel's defense chiefs was that by conducting underground operations in Egypt its military regime could be shown to be insufficiently reliable. Consequently it was hoped for that the British decision to leave Egypt would be reconsidered. The covert network tasked with conducting the attacks in Egypt consisted of two operational cells: one cell in Alexandria and another one in Cairo. Command and control of these cells came from Israeli emissaries which can be viewed as a third cell. The covert affiliation network conducting this operation can therefore be seen to consist of three cells of varying size. After some initial operations the Alexandria cell was detected by Egyptian intelligence and through observation and interrogation the Cairo cell members were also uncovered and arrested. This incident illustrates the importance of being able to evaluate several different possible cell structures *before* conducting and creating an underground network. We will explicitly analyze an explicit but hypothetical example of a covert organization wishing to conduct an attack in Example 5.1 taken from Frantz and Carley [2005].

Many current covert organizational structures can be seen to consist of cells organized in one of several standard forms: a star, a path or a hybrid structure [Arquilla and Ronfeldt, 2001]. For instance Mishal and Rosenthal [2005] present several topological examples in case of Islamic terrorist organizations such as Hamas star-like compart-

mentalization and Hezballah's infiltration of operatives into Israel according to path-like structures. More formally Frantz and Carley [2005] discuss a characterization of cellular networks. It is argued that often each cell in the network forms a clique, i.e., everybody in the cell is connected to everybody else in the cell. The choice of adopting cellular structures clearly is derived from maintaining secrecy and informational scrutiny. Assigning cell leaders and selecting their interaction topology reflects the desired span of control: central in case of a star topology and becoming more decentralized in case of a path, ending up in a hybrid structures. In this chapter we will formalize these basic organizational structures of covert affiliation networks as they can serve as a benchmark for the analysis of more advanced affiliation networks. Thus we will explicitly define the star and path structures consisting of cells that are cliques. In addition we analyze a hybrid structure, called a semi-complete network, consisting of a ring of cells whose leaders are all interconnected. First we will characterize the total distance for the one-mode projections of such affiliation networks. Subsequently we evaluate the secrecy, information and total performance measure for the one-mode projection of these three standard covert affiliation structures. Based on these covert affiliation network indicators we discuss optimality within the class of hypertrees and present a procedure to restructure the affiliation network structure while improving the trade-off performance. Using this procedure we prove that uniform star affiliation networks are optimal in balancing secrecy and information.

Section 5.2 discusses theoretical preliminaries and provides measures that capture the notions of secrecy and information in covert organizations. In addition an example of a covert organization is presented to illustrate the mathematical notation. Section 5.3.1 studies total distance of one-mode projections of several basic hypergraphs. The computation of the total distance is simplified by use of a proposition relating the total distance in a covert affiliation network to its cell-shrinked version. The performance with regard to the information versus secrecy tradeoff of the star, path and a hybrid affiliation structure is analyzed in Section 5.3.2, and we compare their performance to that of the example introduced previously. In addition we will show in Section 5.4 that among all hypertrees of given order and size organizing the affiliation network according to a star is optimal in balancing information and secrecy.

5.2 Preliminaries

A player $i \in N$ that is a member of more than one cell in affiliation network H, i.e., a player i such that $|X(\{i\})| \geq 2$, is called a cell leader. We define the set of cell leaders in H by $L(H)$. The class of connected affiliation networks in which each two cells have at most one player in common is denoted by $\mathbb{H}(N) = \{(N, X) \in \mathbb{C}(N) | \ |A \cap B| \leq 1 \text{ for all } A, B \in X\}$. We denote the class of all r-uniform hypergraphs in $\mathbb{H}(N)$ of size c by $\mathbb{H}_r^c(N)$, the class of all hypertrees in $\mathbb{H}(N)$ of size c by $\mathbb{H}_{tree}^c(N)$ and the class of all r-uniform hypertrees in $\mathbb{H}(N)$ of size c is denoted by $\mathbb{H}_{r-tree}^c(N)$.

Example 5.1 (cf. Frantz et al.)
Consider an organization wishing to carry out an attack with an improvised explosive device. In addition assume that the organization has 16 individuals available to prepare for and conduct such an attack. In preparing the attack several tasks have to be conducted, such as bomb building, delivery of materials and finances, target reconnaissance, target site preparation, etc. The organization adopts a cellular structure by having each cell conduct one such task. We present a *possible* affiliation structure for the preparation and planning of the attack as follows: we label the players 1 through 16 and assume that player 1,2,...,6 constitute the attack cell, player 7,8,...,12 the bomb building cell, player 1 and 7 coordinate between the attack cell and the bomb building cell, player 13 coordinates the finances with player 7, player 16 delivers the materials to player 10, player 14 conducts reconnaissance and delivers information on the target to player 12, and finally player 15 prepares the target site and coordinates this with player 11. Note that this organizational structure corresponds to an example of a covert network as introduced by Frantz and Carley [2005]. The hypergraph corresponding to this organization is denoted by $H_{ex} = (N, X)$ with $N = \{1, 2, ..., 16\}$ and,

$$X = \{A_1, A_2, ..., A_7\}$$

with cells $A_1 = \{7, 8, 9, 10, 11, 12\}$, $A_2 = \{7, 13\}$, $A_3 = \{10, 16\}$, $A_4 = \{12, 14\}$, $A_5 = \{11, 15\}$, $A_6 = \{1, 7\}$ and $A_7 = \{1, 2, 3, 4, 5, 6\}$. Clearly $H_{ex} \in \mathbb{H}_{tree}^7$ and $L(H_{ex}) = \{1, 7, 10, 11, 12\}$. The corresponding one-mode projection $g_\perp(H_{ex})$ is presented in Figure 5.1. ◇

Next we formally define several standard affiliation networks representing basic covert network organizational designs. In particular we model a cell in a covert organization as a cell in a hypergraph [Frantz and Carley, 2005], and we consider a star, a path and a hybrid topology [Arquilla and Ronfeldt, 2001].

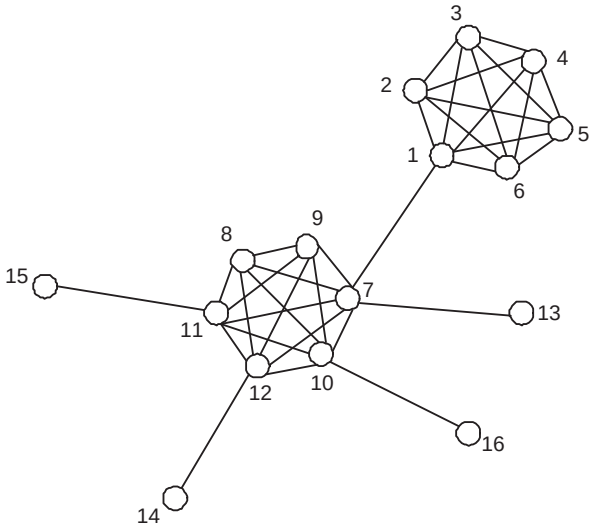


Figure 5.1: One-mode projection of the affiliation network of Example 5.1.

Let $H = (N, X) \in \mathbb{H}_r^c(N)$ be a hypergraph such that $X = \{A_i\}_{i=1}^c$, $c \geq 2$.
The hypergraph H is called an *r-star* , denoted by H_{r-star}^c, if there is a $l \in N$ such that $A_i \cap A_j = \{l\}$ for all $i, j \in \{1, ..., c\}$ with $i \neq j$. Observe that $|L(H_{r-star}^c)| = 1$.

The hypergraph H is called an *r-path*, denoted by H_{r-path}^c , if $|A_i \cap A_j| = 1$ if and only if $j = i + 1$ with $i \in \{1, ..., c - 1\}$. Obviously $|L(H_{r-path}^c)| = c - 1$.

For $c \geq 3$, the hypergraph H is called an *r-ring*, denoted by H_{r-ring}^c, if $|A_i \cap A_j| = 1$ if and only if $j = i + 1$ with $i \in \{1, ..., c - 1\}$ or $i = c$ and $j = 1$. Observe that $|L(H_{r-ring}^c)| = c$.

Finally we introduce a hybrid affiliation network in which cell leaders have an active coordinating role. We do this by considering a ring structure where all cell leaders connect in one additional cell.

Consider $H = (N, X) \in \mathbb{C}(N)$ of size $c+1, c \geq 3$, with $X = \{A_i\}_{i=1}^{c+1}$. The hypergraph H is called *r-semicomplete* , denoted by $H_{r-semicomp}^{c+1}$, if it satisfies the following two properties:

(i) $(N, \{A_i\}_{i=1}^c)$ is a r-ring,

(ii) $L((N, \{A_i\}_{i=1}^c)) = A_{c+1}$.

Note that typically $H_{r-semicomp}^{c+1} \notin \mathbb{H}(N)$.

In Table 5.1 we indicate the order and size of the one-mode projection graphs for the three standard affiliation networks.

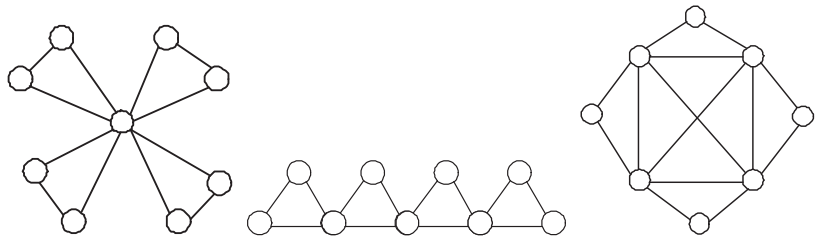


Figure 5.2: One-mode projections of H^4_{3-star} (left), H^4_{3-path} (middle) and $H^5_{3-semicomp}$(right).

$g_\perp(H) = (N, E)$	$\lvert N\rvert = n$	$\lvert E\rvert = m$
$H = H^c_{r-star}$	$c(r-1)+1$	$\frac{cr(r-1)}{2}$
$H = H^c_{r-path}$	$c(r-1)+1$	$\frac{cr(r-1)}{2}$
$H = H^{c+1}_{r-semicomp}$	$c(r-1)$	$\frac{c(r(r-1)+c-3)}{2}$

Table 5.1: Order and size of the three one-mode projections of standard hypergraphs.

Finally we recall the definitions of measures specifically designed for the analysis of the interaction structure of covert networks as introduced in chapter 3. The average information performance $I(g)$ of a network $g \in \mathbb{G}(N)$ with $|N| = n$ is defined as the normalized reciprocal of the total distance $T(g)$,

$$I(g) = \frac{n(n-1)}{T(g)}. \tag{5.1}$$

It follows that $0 \leq I(g) \leq 1$. The secrecy performance $S(g)$ of a network $g \in \mathbb{G}(N)$ with $|N| = n$ and size m is given by

$$S(g) = \frac{n^2 - n - 2m}{n^2} \tag{5.2}$$

with $0 \leq S(g) \leq 1$. We showed in chapter 3 that $S(g)$ represents the expected fraction of the network that 'survives' given an uniform exposure probability distribution and the assumption that upon exposure of individual i all individuals with which he is connected are also exposed. Moreover it was argued on the basis of multi-objective optimization and bargaining theory that a covert organization that wishes to balance the tradeoff between secrecy and information does best by adopting a network g that maximizes the performance measure μ, defined by

$$\mu(g) = S(g)I(g). \tag{5.3}$$

5.3 One-mode Projection Analysis

5.3.1 Total distance

Computing the total distance of the one-mode projections $g_\perp(H)$ corresponding to a hypergraph H can be cumbersome. We will prove that to compute the total distance in the one-mode projection of r-uniform hypertrees one only needs to compute the total distances of a certain subset of its players. This subset arises from the so-called corresponding 'cell-shrinked' version of the hypertree, which will be explained next.

The *cell shrinked* graph $g^-(H)$ corresponding to an r-uniform hypertree $H = (N, X) \in \mathbb{H}^c_{r-tree}(N)$ is defined as follows. For each $A \in X$ such that $|A \cap L(H)| = 1$ we take exactly one *representative* $j_A \in A \setminus L(H)$ and define $R(H) = \{j_A | A \in X, |A \cap L(H)| = 1\}$. We set $LR = L(H) \cup R(H)$ and define $g^-(H)$ as the LR-induced subgraph of $g_\perp(H)$. See Figure 5.3 below for an illustration.

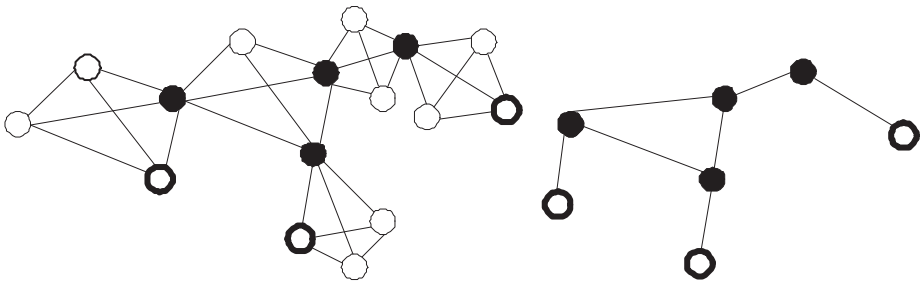


Figure 5.3: One-mode projection $g_\perp(H)$ (left) and its cell shrinked version $g^-(H)$ (right), the leaders are represented by solid dots and the representatives by bold line dots.

We relate the total distance in an r-uniform hypertree $H = (N, X)$ to the total distance of the players in its corresponding cell-shrinked version. For this aim define $n_A = |A \cap LR|$ for all $A \in X$ and let

$$w_k(H) = 1 + \sum_{A \in X : k \in A} \frac{r - n_A}{n_A}$$

for all $k \in LR$. Note that $n_A = 2$ if $|L(H) \cap A| = 1$, and that $n_A \geq 2$ otherwise.

Proposition 5.3.1 *Let $H = (N, X) \in \mathbb{H}^c_{r-tree}$. Set $g^-(H) = (LR, E)$. Then*

(i) For all $j \in N \setminus LR$ and $A \in X$ the unique event such that $j \in A$ it holds that $l_j(g_\perp(H)) = \frac{n-r}{n_A} + \frac{1}{n_A} \sum_{k \in LR \cap A} l_k(g_\perp(H))$,

(ii) $T(g_\perp(H)) = \sum_{k\in LR} w_k(H) l_k(g_\perp(H)) + (n-r)\sum_{A\in X} \frac{r-n_A}{n_A}$.

Proof:

(i) Consider $j \in N \setminus LR$ and let $A \in X$ be the unique event such that $j \in A$. Let $k \in LR \cap A$ and define $N_k(j) = \{z \in N \setminus \{k\} | l_{kz}(g_\perp(H)) < l_{jz}(g_\perp(H))\}$. It readily follows that

$$l_j(g_\perp(H)) = l_k(g_\perp(H)) + |N_k(j)|.$$

Therefore,

$$l_j(g_\perp(H)) = \frac{1}{n_A}\sum_{k\in A\cap LR}(l_k(g_\perp(H)) + |N_k(j)|) = \frac{1}{n_A}\sum_{k\in A\cap LR} l_k(g_\perp(H)) + \frac{n-r}{n_A}.$$

(ii) Note that

$$\begin{aligned}
T(g_\perp(H)) &= \sum_{k\in LR} l_k(g_\perp(H)) + \sum_{j\in N\setminus LR} l_j(g_\perp(H)) \\
&= \sum_{k\in LR} l_k(g_\perp(H)) + \sum_{A\in X}\sum_{j\in A\setminus LR} l_j(g_\perp(H)) \\
&= \sum_{k\in LR} l_k(g_\perp(H)) + \sum_{A\in X}(r-n_A)[\frac{n-r}{n_A} + \frac{1}{n_A}\sum_{k\in LR\cap A} l_k(g_\perp(H))] \\
&= \sum_{k\in LR} l_k(g_\perp(H)) + (n-r)\sum_{A\in X}\frac{r-n_A}{n_A} + \sum_{A\in X}\frac{r-n_A}{n_A}\sum_{k\in LR\cap A} l_k(g_\perp(H)) \\
&= \sum_{k\in LR} l_k(g_\perp(H)) + (n-r)\sum_{A\in X}\frac{r-n_A}{n_A} + \sum_{k\in LR} l_k(g_\perp(H))\sum_{A\in X, k\in A}\frac{r-n_A}{n_A} \\
&= \sum_{k\in LR}\{1 + \sum_{A\in X, k\in A}\frac{r-n_A}{n_A}\} l_k(g_\perp(H)) + (n-r)\sum_{A\in X}\frac{r-n_A}{n_A} \\
&= \sum_{k\in LR} w_k(H) l_k(g_\perp(H)) + (n-r)\sum_{A\in X}\frac{r-n_A}{n_A}.
\end{aligned}$$

Where the third equality follows from (i). □

Proposition 5.3.2 *Let $H = (N, X) \in \mathbb{H}^c_{r-tree}$ be such that $n_A = 2$ for all $A \in X$. Then*

$$T(g_\perp(H)) = (r-1)\sum_{k\in LR} w_k(H) l_k(g^-(H)) + (n-r)\sum_{A\in X}\frac{r-n_A}{n_A}. \tag{5.4}$$

Proof:

Since $n_A = 2$ for all $A \in X$ it holds that $g^-(H)$ is a tree. Hence, since every cell of $g_\perp(H)$ contains r players it follows that

$$l_i(g_\perp(H)) = (r-1) l_i(g^-(H)) \quad \text{for all} \quad i \in LR.$$

and the result follows from Proposition 5.3.2(ii). □

For the three standard types of hypergraphs the total distances of their one-mode projections are provided in the lemma below.

Lemma 5.3.1

(i) $T(g_\perp(H^c_{r-star})) = c(r-1)[r + 2(c-1)(r-1)]$

(ii) $T(g_\perp(H^c_{r-path})) = c(r-1)(cr + \frac{1}{3}c^2r + \frac{4}{3} - c - \frac{1}{3}r - \frac{1}{3}c^2)$

(iii) $T(g_\perp(H^{c+1}_{r-semicomp})) = c(r-1)(3cr + 7 - 5c - 4r)$

Proof:

(i) Consider $H = H^c_{r-star}$ and let $i \in N$ be the unique leader of H. Clearly i has distance 1 to all other $c(r-1)$ nodes, i.e.,

$$l_i(g_\perp(H)) = c(r-1).$$

The nodes $j \in N \setminus \{i\}$ have distance 1 to each other member of the cell they belong to and distance 2 to the remaining nodes, hence

$$l_j(g_\perp(H)) = (r-1) + 2(c-1)(r-1)$$

for all $j \in N \setminus \{i\}$. Consequently

$$T(g_\perp(H)) = c(r-1) + c(r-1)[(r-1) + 2(c-1)(r-1)]$$

and the result follows.

(ii) Consider $H = H^c_{r-path} = (N, X)$. Since $n_A = 2$ for all $A \in X$ we can use the result in Proposition 5.3.2 to determine $T(g_\perp(H))$. Let $g = g^-(H) = (LR, E)$ with $LR = L(H) \cup R(H)$. Clearly $|L(H)| = c - 1$ and $|R(H)| = 2$. Then

$$\begin{aligned}
T(g_\perp(H)) &= (r-1)\sum_{k\in LR} w_k(H)l_k(g) + (n-r)\sum_{A\in X}\frac{r-n_A}{n_A} \\
&= (r-1)\sum_{k\in L(H)} w_k(H)l_k(g) + (r-1)\sum_{k\in R(H)} w_k(H)l_k(g) + (n-r)c(\frac{r-2}{2}) \\
&= (r-1)\sum_{k\in L(H)} (r-1)l_k(g) + (r-1)\sum_{k\in R(H)} \frac{r}{2}l_k(g) + \frac{1}{2}c(c-1)(r-2)(r-1) \\
&= (r-1)^2\sum_{k\in L(H)} l_k(g) + \frac{r(r-1)}{2}\cdot 2\cdot\frac{c(c+1)}{2} + \frac{1}{2}c(c-1)(r-2)(r-1) \\
&= (r-1)^2[\frac{c(c+1)(c+2)}{3} - c(c+1)] + \frac{1}{2}rc(r-1)(c+1) + \frac{1}{2}c(c-1)(r-2)(r-1)
\end{aligned}$$

and the result follows. Note that the last equality follows from the fact that $T(g) = \frac{c(c+1)(c+2)}{3}$ as is derived in Lemma 3.2.1.

(iii) Consider $H = H^{c+1}_{r-semicomp} = (N, X)$. Take $i \in L(H)$. Clearly

$$\begin{aligned} l_i(g_\perp(H)) &= 1 \cdot (2(r-2)+c-1) + 2(c(r-1)-1-(2(r-2)+c-1)) \\ &= 2(c+1)r + 6 - 4r - 3(c+1). \end{aligned}$$

Now take $j \in N \setminus L(H)$. Then

$$\begin{aligned} l_j(g_\perp(H)) &= 1 \cdot (r-1) + 2(c-2+2(r-2)) + 3(c(r-1)-1-(r-1+c-2+2(r-2))) \\ &= 3(c+1)r - 4(c+1) - 7r + 9. \end{aligned}$$

Then

$$\begin{aligned} T(g_\perp(H)) &= \sum_{i \in L(H)} l_i(g_\perp(H)) + \sum_{j \in N \setminus L(H)} l_j(g_\perp(H)) \\ &= c[2(c+1)r + 6 - 4r - 3(c+1)] + c(r-2)[3(c+1)r - 4(c+1) - 7r + 9] \end{aligned}$$

and the result follows. □

5.3.2 Covert affiliation network performance

In analyzing covert affiliation networks their one-mode projection graphs can be seen to represent the interaction structure among the members of the organization. In this section we analyze the performance measure μ for the one-mode projections of the three basic covert affiliation networks H^c_{r-star}, H^c_{r-path} and $H^{c+1}_{r-semicomp}$.

From the definition of the information performance measure I as given in equation (5.1) together with Table 5.1 and Lemma 5.3.1 one readily derives

Lemma 5.3.2

(i) $I(g_\perp(H^c_{r-star})) = \frac{c(r-1)+1}{2cr-2c-r+2}$

(ii) $I(g_\perp(H^c_{r-path})) = \frac{3(c(r-1)+1)}{3cr+c^2r+4-3c-r-c^2}$

(iii) $I(g_\perp(H^{c+1}_{r-semicomp})) = \frac{c(r-1)-1}{3cr-5c-4r+7}$

From the definition of the secrecy measure S in equation 5.2 and Table 5.1 together with Lemma 5.3.3 we find

Lemma 5.3.3

(i) $S(g_\perp(H^c_{r-star})) = \frac{c(c-1)(r-1)^2}{(c(r-1)+1)^2}$

(ii) $S(g_\perp(H^c_{r-path})) = \frac{c(c-1)(r-1)^2}{(c(r-1)+1)^2}$

(iii) $S(g_\perp(H^{c+1}_{r-semicomp})) = \frac{(r-2)(r(c-1)-2)}{c(r-1)^2}$

In addition we present an asymptotic analysis in Table 5.2. From Lemma 5.3.2(i)

H	H^c_{r-star}	H^c_{r-path}	$H^{c+1}_{r-semicomp}$
$\lim_{r\to\infty} I(g_\perp(H))$	$\frac{c}{2c-1}$	$\frac{3c}{c^2+3c-1}$	$\frac{c}{3c-4}$
$\lim_{c\to\infty} I(g_\perp(H))$	$\frac{1}{2}$	0	$\frac{r-1}{3r-5}$
$\lim_{r\to\infty} S(g_\perp(H))$	$\frac{c-1}{c}$	$\frac{c-1}{c}$	$\frac{c-1}{c}$
$\lim_{c\to\infty} S(g_\perp(H))$	1	1	$\frac{r(r-2)}{(r-1)^2}$

Table 5.2: Asymptotic analysis of the information and secrecy performance measure.

and (ii) it follows that for sufficiently many cells, the star affiliation network outperforms the path with regard to information performance. Intuitively this is clear: the distance between cells in a star affiliation network is maximally 2 whereas it becomes increasingly more difficult to reach other cells in case of a path affiliation structure. However, it can also be seen that in case of a small number of cells the semi-complete hypergraph may outperform the star. From Lemma 5.3.3 it can be seen that in case of a low value of r, i.e., small cells, the star affiliation network outperforms the path and semi-complete hypergraph with regard to secrecy. From Table 5.2 it can also be seen that the star network outperforms the other networks asymptotically.

From the definition of the performance measure, Lemma 5.3.2 and Lemma 5.3.3 we find

Theorem 5.3.1

(i) $\mu(g_\perp(H^c_{r-star})) = \frac{c(c-1)(r-1)^2}{(c(r-1)+1)(2cr-2c-r+2)}$

(ii) $\mu(g_\perp(H^c_{r-path})) = \frac{3c(c-1)(r-1)^2}{(c(r-1)+1)(3cr+c^2r+4-3c-r-c^2)}$

(iii) $\mu(g_\perp(H^{c+1}_{r-semicomp})) = \frac{(c(r-1)-1)(r-2)(r(c-1)-2)}{c(r-1)^2(3cr-5c-4r+7)}$

We compare the total performance of the star, path and semi-complete covert network affiliation structures in Figure 5.4

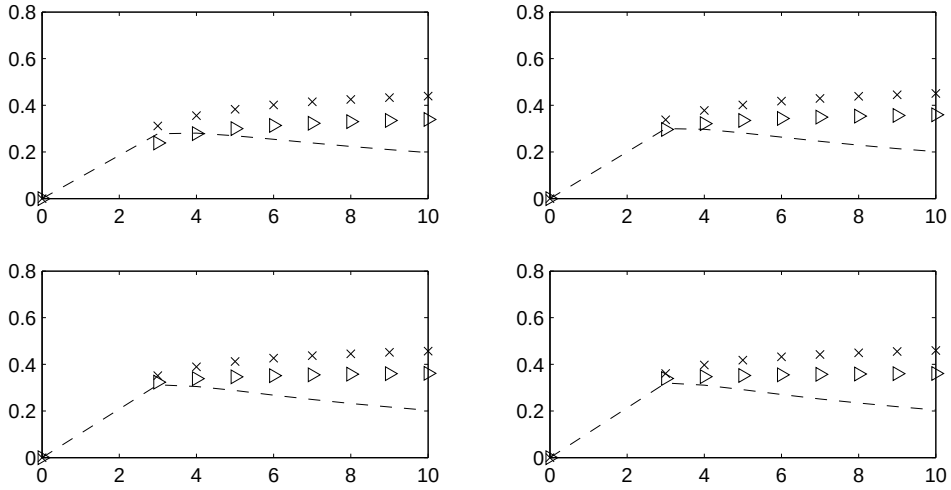


Figure 5.4: Performance measure μ of H^c_{r-path} (–), H^c_{r-star} (x) and $H^{c+1}_{r-semicomp}$ (Δ) as a function of the number of cells c (horizontal axis) and the number of nodes r per cell. Top left: r=3, top right: r=4, down left: r=5, down right: r=6.

It can be seen that the star affiliation network outperforms the other basic affiliation networks.

Example 5.2

In Example 5.1 we considered an organization wishing to carry out an attack. Seven tasks were divided among as many cells. We compare the information, secrecy and trade-off performance of the affiliation network H_{ex} as presented in Example 5.1 with that of comparable basic affiliation networks. For this purpose we consider a star and path network consisting of 7 cells, i.e., H^7_{3-star} and H^7_{3-path}, and since semi-complete networks have an additional cell of leaders, $H^8_{3-semicomp}$. Both the star and semi-complete affiliation

	$I(g_\perp(H))$	$S(g_\perp(H))$	$\mu(g_\perp(H))$
$H = H^7_{3-star}$	0.56	0.75	0.42
$H = H^7_{3-path}$	0.32	0.75	0.24
$H = H^8_{3-semicomp}$	0.56	0.57	0.32
$H = H_{ex}$	0.44	0.66	0.29

Table 5.3: A comparison of the information, secrecy and total trade-off performance in the setting of Example 5.1.

structures outperform the actual structure, whereas the path affiliation network performs worse. This leads to the conclusion that, assuming that secrecy and information are

the most decisive parameters in conducting such a covert operation, the organizational structure could be improved upon. ◇

5.4 On optimal affiliation networks

The results in Section 5.3 indicate that an r-star hypergraph is an adequate affiliation network for covert organizations in terms of secrecy and information performance. This leads us to investigate the performance of the star hypergraph affiliation network H^c_{r-star} in more detail. In this section we will show that the r-star outperforms all comparable hypertrees with the same number of cells and of the same order. Before we formally state and prove this assertion in Theorem 5.4.1 we first describe a 'tree-to-star' transformation procedure.

Consider a hypertree $H = (N, X) \in \mathbb{H}^c_{tree}$, consisting of c cells, of possibly different size. With $j, k \in N$, $k \neq j$, define

$$N_k(j) = \{i \in N | l_{ki}(g_\perp(H)) < l_{ji}(g_\perp(H))\}$$

as the set of nodes closer to k than to j in the one-mode projection of H. The 'tree-to-star' transformation consists of the following five steps.

(1) Select $A \in X$ such that $|A \cap L(H)| > 1$. Note if H is not a star, this is possible.

(2) Set $A \cap L(H) = \{a_1, ..., a_t\}$.

(3) Set $X_1 = X$.

(4) For $i = 2$ to t do

  (i) set $B_i = X(\{a_i\}) \setminus \{A\}$,

  (ii) for all $C \in B_i$ let $\bar{C} = (C \setminus \{a_i\}) \cup \{a_1\}$,

  (iii) let $\bar{B}_i = \{\bar{C} | C \in B_i\}$,

  (iv) set $X_i = (X_{i-1} \setminus B_i) \cup \bar{B}_i$.

(5) Set $X = X_t$. If $\{A \in X || A \cap L(H)| > 1\} \neq \emptyset$ return to step 1, otherwise stop[1].

This procedure results in a hypergraph whose one-mode projection equals a star graph, possibly with cells of different sizes. We illustrate this procedure by an example.

[1]The algorithm stops since each iteration the number of cell leaders is reduced.

Example 5.3:
Let $H = (N, X)$ with $N = \{1, 2, ..., 16\}$ and

$$X = \{A_1, ..., A_5\}$$

with cells $A_1 = \{1, 2, 3, 15, 16\}$, $A_2 = \{3, 4, 5, 11, 14\}$, $A_3 = \{5, 6, 7\}$, $A_4 = \{7, 8, 9, 10\}$ and $A_5 = \{11, 12, 13\}$ (see Figure 4.5 top left for $g_\perp(H)$). Clearly $L(H) = \{3, 5, 7, 11\}$. In step 1 select $A = A_2$ with $A_2 \cap L(H) = \{5, 11, 3\}$ and set $a_1 = 5$, $a_2 = 11$ and $a_3 = 3$. Since $X(\{11\}) = \{A_2, A_5\}$ it follows that $B_2 = \{A_5\}$ (step 4i) and we obtain $\bar{A}_5 = \{5, 12, 13\}$, $\bar{B}_2 = \{\{5, 12, 13\}\}$ and $X_2 = \{A_1, A_2, A_3, A_4, \{5, 12, 13\}\}$ (in Figure 4.5 top right the one-mode projection of this intermediate hypergraph is presented). Similarly we find $\bar{B}_3 = \{\{1, 2, 5, 15, 16\}\}$ and $X_3 = \{\{1, 2, 5, 15, 16\}, A_2, A_3, A_4, \{5, 12, 13\}\}$. Now $A_3 \cap L(H) = \{5, 7\}$, hence we return to step 1 and repeat. Choosing $a_1 = 5$ and $a_2 = 7$ results in the star $H' = (N, X')$ with

$$X' = \{\{3, 4, 5, 11, 14\}, \{1, 2, 5, 15, 16\}, \{5, 6, 7\}, \{5, 8, 9, 10\}, \{5, 12, 13\}\}.$$

In Figure 5.5 bottom the resulting one-mode projection $g_\perp(H')$ is presented. ◇

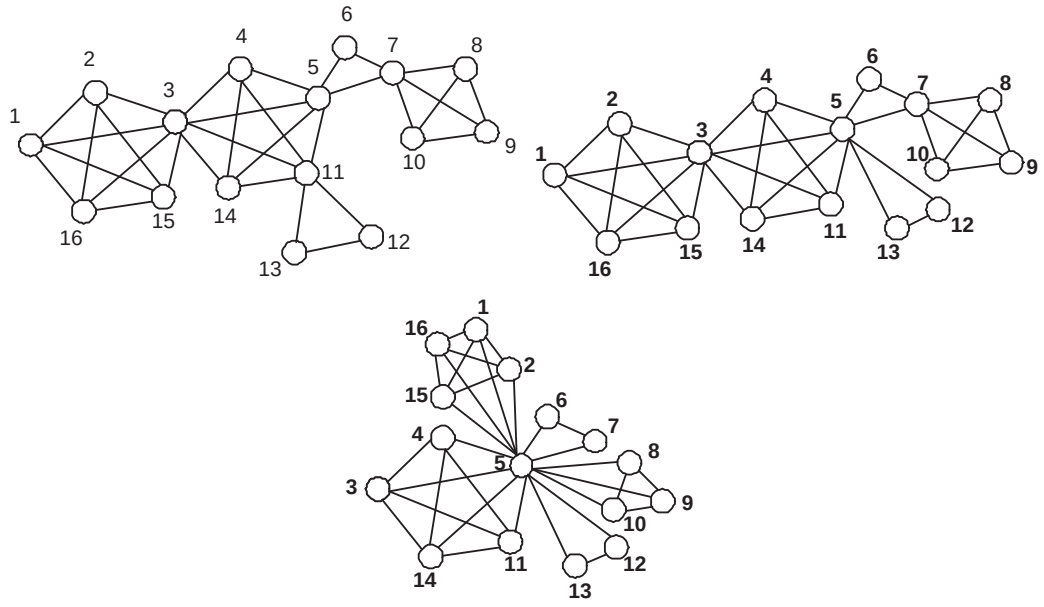


Figure 5.5: Illustration of the 'tree-to-star' transformation procedure in Example 5.3.

We now show that the r-star hypergraph maximizes the performance μ among all fixed size and order hypertrees by first showing that each iteration in the 'tree-to-star'

transformation procedure increases the value of μ for the corresponding hypergraph and secondly that among all star affiliation networks with cells of different sizes r-uniform ones are optimal.

Theorem 5.4.1 *$\mu(g_\perp(H^c_{r-star})) \geq \mu(g_\perp(H))$ for all $H \in \mathbb{H}^c_{tree}$ of order $n = (r-1)c+1$.*

Proof:
Let $H = (N, X) \in \mathbb{H}^c_{tree}$ with $|N| = (r-1)c+1$ and apply the 'tree-to-star' transformation procedure. Denote the resulting star hypergraph by $H' = (N, X')$. Note that every iteration of steps 4 reduces the total distance in the corresponding one-mode projections (in fact within each iteration i the total distance reduces by $2|N_{a_i}(a_1)| \cdot |N_{a_1}(a_i)|$). Since the size and order of the one-mode projection remain constant during the transformation it follows that $\mu(g_\perp(H')) > \mu(g_\perp(H))$.

Let $g_\perp(H') = (N, E)$ with $|E| = m$. Note that there are exactly m pairs ij such that $l_{ij}(g_\perp(H')) = 1$ and hence $\binom{n}{2} - m$ pairs ij with $l_{ij}(g_\perp(H')) = 2$. Then,

$$T(g_\perp(H')) = 2(m + 2(\binom{n}{2} - m)) = 2n(n-1) - 2m.$$

Therefore

$$\mu(g_\perp(H')) = \frac{(n^2-n)(n^2-n-2m)}{n^2(2n^2-2n-2m)}$$

and consequently $\frac{\partial \mu}{\partial m} = -\frac{1}{2}\frac{(n-1)^2}{(n^2-n-m)^2} < 0$. Since m is minimal for H^c_{r-star} it follows that $\mu(g_\perp(H^c_{r-star})) \geq \mu(g_\perp(H'))$. □

Theorem 5.4.1 shows that organizing cells in a r-star topology does well in balancing the trade-off between information and security. Clearly H^c_{r-star} does not exist if $\frac{n-1}{c}$ is not integer. However Theorem 5.4.1 can easily be extended to these cases by considering the star hypergraph 'closest' to H^c_{r-star}: stars consisting of cells which differ by at most one node.

5.5 Affiliation Heterogeneity

In chapter 3 we introduced a homogenous covert network model based on the trade-off between secrecy and information. In chapter 4 this model was extended by considering secrecy heterogeneity (Section 4.3) and information heterogeneity in case of star networks (Section 4.4). In this chapter we introduced covert *affiliation* networks and analyzed their one-mode projection with respect to homogeneous secrecy and information. Here

we present a first approach to secrecy and information *heterogeneity* of covert affiliation networks. To model information heterogeneity in covert affiliation networks we introduce the concept of a *weighted* one-mode projection of an affiliation network. In addition we introduce a heterogeneous secrecy measure for covert affiliation networks by adjusting the probability of exposure.

In Section 5.3.2 we applied the homogeneous information and secrecy measure to the analysis of the one-mode projection of covert affiliation networks. In this section we present an extension on the information performance by taking the amount of information exchange that occurs between participants in covert cells explicitly into account. Clearly individuals $i, j \in N$ engaged in affiliation network $H = (N, X)$ can communicate through their common participation in all events belonging to $X(\{i\}) \cap X(\{j\})$. As already noted, a natural representation of the communication structure among individuals engaged in an affiliation network $H = (N, X)$ is given by the corresponding one-mode projection $g_\perp(H) = (N, E)$. In Section 4.3 we introduced a weighting function for covert networks, $c : E \to [1, \delta_I]$ to represent the amount of information exchange between vertices such that $c_{ij} > c_{kl}$ with $ij, kl \in E$ implies that the amount of information exchanged between individuals (terror cells, military units, human traffickers) i and j is higher than the amount of information exchanged between individuals k and l. Given affiliation network $H = (N, X)$ and its one-mode projection $g_\perp(H) = (N, E)$ we define

$$c_{ij}(H) = |X(\{i\}) \cap X(\{j\})| \quad \text{for all} \quad i, j \in N \quad \text{such that} \quad ij \in E, \tag{5.5}$$

i.e., the amount of information exchange between individual i and j is proportional to the number of events (cells) they both are engaged in.

To define the heterogeneous information measure for covert affiliation networks we incorporate heterogeneity with respect to the nature of interaction as in [Lindelauf et al., 2009b]. Therefore we define *resistances* on the edges of the one-mode projection of the affiliation network. Let $H = (N, X)$ with $g_\perp(H) = (N, E)$, the resistance of edge $ij \in E$ is defined to be the reciprocal of the measure for heterogeneous information exchange, i.e., $r_{ij}(H) = \frac{1}{c_{ij}(H)}$ for all $ij \in E$. We denote a path between player i and j in graph $g_\perp(H)$ by $P_{ij}(H)$. The 'distance' between player i and j is defined as the shortest *resistance-weighted* path between i and j:

$$l_{ij}(H) = min_{P_{ij}(H)} \sum_{kl \in P_{ij}(H)} r_{kl},$$

and the associated total distance is $T(H) = \sum_{i,j \in N \times N} l_{ij}(H)$.

The heterogeneous information measure $I(H)$ of hypergraph $H = (N, X)$ is defined by

$$I(H) = \frac{\frac{1}{|X|}n(n-1)}{T(H)}. \tag{5.6}$$

In chapter 3 and subsequent chapters it has been explained that the secrecy measure reflects the expected fraction of the network that survives given that members of the organization are detected according to a realistically chosen probability distribution. Among others the secrecy measure depends on the probability of exposure of individual $i \in N$. To define the heterogeneous secrecy measure for covert affiliation networks we adjust the choice of exposure probability α as follows. Let $H = (N, X)$, define

$$\alpha_i(H) = \frac{|X(\{i\})|}{\sum_{j\in N}|X(\{j\})|} \quad \text{for all} \quad i \in N. \tag{5.7}$$

This choice of definition can be motivated as follows. The more cells a player is engaged in, the more likely it is that he will be exposed as a member of the covert affiliation network. In addition to the probability of exposure the secrecy measure also depends on the fraction of individuals that are exposed if any individual is detected. In the context of affiliation networks we assume that if individual i is detected he potentially exposes all those individuals with whom he participates in cells. That is, we set $u_i(H) = 1 - \frac{d_i(g_\perp(H))+1}{n}$.

The heterogeneous secrecy measure $S(H)$ of hypergraph $H = (N, X)$ is defined by

$$\begin{aligned} S(H) &= \sum_{i\in N} \frac{|X(\{i\})|}{\sum_{j\in N}|X(\{j\})|} \cdot \frac{n - d_i(g_\perp(H)) - 1}{n} \\ &= \frac{n-1}{n} - \frac{1}{n}\sum_{i\in N} \frac{|X(\{i\})|d_i(g_\perp(H))}{\sum_{j\in N}|X(\{j\})|}. \end{aligned}$$

Finally given covert affiliation network $H = (N, X)$ we set $\mu(H) = I(H)S(H)$.

We illustrate the use of this heterogenous affiliation measure with the Hamas operation to target Israel by use of rockets, a covert operation Hamas conducted during the 2008 Cast Lead conflict.

Example 5.4:
Hamas operates in a context of opportunities and constraints, conflicting interests, and cost-benefit considerations, and is attentive to the fluctuating needs and desires of the Palestinian population and cognizant of power relations and political feasibility [Mishal

and Rosenthal, 2005]. It is headed by a political bureau with representatives for military affairs, foreign affairs, finance, propaganda and internal security [Zuhur, 2008]. However, Hamas is a loosely structured organization, and has some elements working clandestinely [Levitt, 2004]. It is known that Hamas set up a complex system, ranging from smuggling components into Gaza to identifying and preparing launch sites [Cohen and White, 2009], [Ben-David, 2009]. To conduct such operations individuals (or teams) were assigned to cells each conducting a specific task. In general such assignments are unknown to the opponent to ensure the necessary secrecy of the operation. The organizational form of the operations Hamas conducts is not easily identified due to their covert nature.

Hamas is an example of an organization that conducts operations which can be viewed from the perspective of affiliation networks. Its decision making and leadership is effectively divided between Damascus and Gaza (ignoring the less influential West Bank leadership and those in Israeli jails). Operation Cast Lead, Israel's 2008/9 air and ground campaign into Gaza, provided a real test of the military wing of Hamas, the Izz al-Din al-Qassam (IDQB) brigades. During that operation Hamas combat forces were essentially made up of two elements: rocket and mortar forces and defensive formations organized to defend Gaza [Cohen and White, 2009]. Here we present and analyze such a stylized rocket operation.

Consider a set of ten players $N = \{1, 2, ..., 10\}$ (which could either be individuals or teams) tasked to conduct a rocket operation. Operationally they have to acquire the necessary materials by smuggling them into the area of operations (A), assemble and store the rockets (B), identify and prepare the launch site (C) and conduct the attack (D). Thus the group has to decide how to allocate the individuals/teams in N to cells, each responsible for one of those four different tasks. Consider two possible affiliation structures $H_1 = (N, X)$ and $H_2 = (N, Y)$ with

$$\begin{aligned} X &= \{\{1,2,3,4\},\{4,5,6,7\},\{7,8,9\},\{9,10\}\} \\ Y &= \{\{1,2,3,4,5,6,7\},\{1,2,3,4,5,6,8\}, \\ &\quad \{1,2,3,4,5,6,9\},\{1,2,3,4,5,6,10\}\}. \end{aligned}$$

The one-mode projections $g_\perp(H_1) = (N, E_1)$ and $g_\perp(H_2) = (N, E_2)$ are shown in Figure 5.6. It holds that $c_{ij}(H_1) = 1$ for all $ij \in E_1$. Let

$$\begin{aligned} B &= \{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{2,3\},\{2,4\}, \\ &\quad \{2,5\},\{2,6\},\{3,4\},\{3,5\}\{3,6\},\{4,5\},\{4,6\},\{5,6\}\} \end{aligned}$$

.

It holds that $c_{ij}(H_2) = 1$ for all $ij \in E_2 \setminus B$, $c_{kl}(H_2) = 4$ for all $kl \in B$.

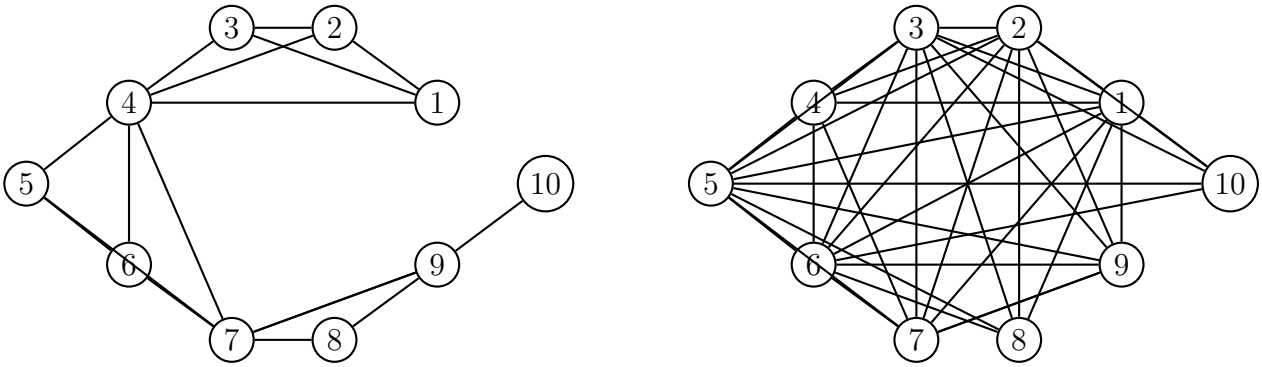


Figure 5.6: One-mode projections $g_\perp(H_1)$ (Left) and $g_\perp(H_2)$ (Right).

We have $I(H_1) = 0,1264$ and $I(H_2) = 0,2830$. Clearly the affiliation structure H_2 outperforms H_1 with respect to information simply because there exist more connections among those individuals due to their common participation in several cells. However this also presents a security risk. We find that $S(H_1) = 0,5462$ and $S(H_2) = 0,0429$. As expected it can be seen that the affiliation structure H_2 does not perform very well with respect to secrecy.

To approximate an optimal affiliation structure consisting of four cells we randomly generate an affiliation network $H = (N, X)$ from the set $\mathbb{H}^c(N)$ with $|N| = 10$ and $c = 4$. We compute the corresponding information measure $I(H)$, secrecy measure $S(H)$ and trade-off measure $\mu(H)$ and plot the secrecy measure (horizontal axis) versus the information measure (vertical axis), see Figure 5.7.

We repeat this procedure 100.000 times and we find that $H_3 = (N, Z)$ with $Z = \{A_1, A_2, A_3, A_4\}$ such that,

$$\begin{aligned} A_1 &= \{1, 2, 4, 5, 7, 8\} \\ A_2 &= \{1, 2, 3, 6, 7, 8, 9, 10\} \\ A_3 &= \{2, 3, 6, 7, 10\} \\ A_4 &= \{1, 4, 5, 6, 8, 10\} \end{aligned}$$

maximizes μ among these 100.000 uniformly generated hypergraphs from the set $\mathbb{H}^c(N)$ with $c = 4$, $|N| = 10$ (see Figure 5.8 for $g_\perp(H_3)$).

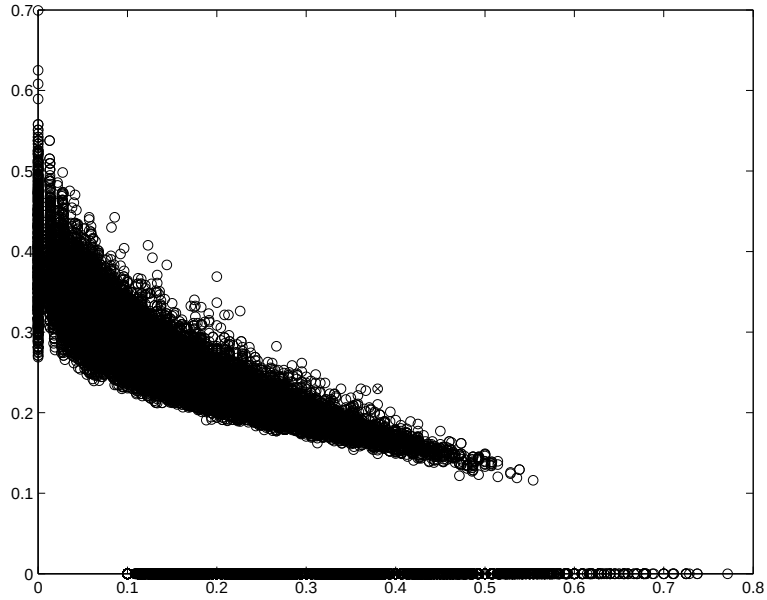


Figure 5.7: $S(H)$ (horizontal axis) and $I(H)$ (vertical axis) of 100.000 randomly generated affiliation networks of order 10 and size 4.

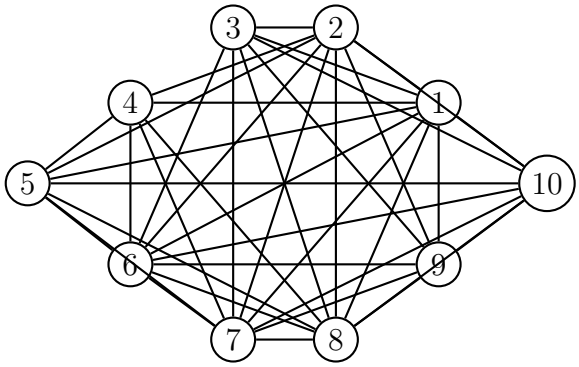


Figure 5.8: One-mode weighted projection $g_{\perp}(H_3)$ of approximate optimal affiliation network consisting of 10 players and 4 cells.

In Table 5.4 we summarize the performance of the affiliation networks presented here.

H	$S(H)$	$I(H)$	$\mu(H)$
$H = H_1$	$0,5462$	$0,1264$	$0,0690$
$H = H_2$	$0,0429$	$0,2830$	$0,0121$
$H = H_3$	$0,3800$	$0,2296$	$0,0872$

Table 5.4: Example affiliation network performance overview.

5.6 Remarks and observations

In this chapter we analyzed the secrecy versus information dilemma every covert organization faces, where we modeled the structure of a covert organization as an affiliation network. The motivation for the affiliation network perspective is because often covert organizations form cells and assign each cell with a certain task of the operation. Only a limited number of cell members are aware of (a limited number of) other cell members, ensuring the necessary secrecy of the operation. The same question as analyzed in the previous chapter springs to mind: 'can we quantitatively measure the quality of an affiliation network in balancing secrecy versus information performance?'.

We modeled covert affiliation networks by their one-mode projection graph. This graph represents the communication structure that exists among the members in the affiliation network (generally it is known that covert cells form so-called mathematical cliques). First we analyzed these one-mode projections using the methodology developed in chapter 3 on homogeneous covert networks and found that among several standard affiliation networks, consisting of sufficiently large cells, the star affiliation structures outperform the other ones. In addition it was shown that the star affiliation networks actually outperform all comparable affiliation networks of the same number of cells and order. It might be argued that the assumptions leading to this result are too restrictive. Therefore we also analyzed covert affiliation networks from a heterogenous perspective by way of an example. We adjusted both the information and secrecy measure by taking the number of cells individuals share into account. By simulation we found approximate optimal heterogeneous covert affiliation networks.

Viewing covert organizations from a affiliation network perspective opens up new avenues of research on such organizations. First because generally much of the (standard) network analysis that is being done considers (undirected) 'normal' networks. Second because due to the nature of covert organizations they tend to form cells that already more or less represent affiliation structures. In addition such covert organizations have

to perform tasks, i.e., they want to conduct an attack. To ensure operation success it is known empirically that covert organizations form redundant cells. Even though we did not explicitly take into account the fact that a covert organization is conducting an operation consisting of tasks, viewing them from an affiliation network perspective is a first approach in implicitly doing so. In chapter 8 we will more extensively analyze covert organizations from the perspective of tasks in projects. Future research combining both these approaches appears to be fruitful in gaining our understanding of the functioning of such organizations, and quantitatively measuring their performance.

Chapter 6

Covert Network Topologies and Resilience

If a man does not keep pace with his companions, perhaps it is because he hears a different drummer. Let him step to the music which he hears, however measured or far away.
- Henry David Thoreau.

6.1 Introduction

The study of criminal and terrorist networks can also benefit from insights obtained by researchers that have begun to unravel the structure and dynamics of many different social, biological and other complex networks [Strogatz, 2001], [Jasny and Ray, 2003] [Newman et al., 2006], [Zacharias et al., 2008]. Typically research on criminal or terrorist networks, i.e., research on covert networks, considers destabilization strategies [Farley, 2003], [Carley, 2006], organizational characterizations [McCormick and Owen, 2000], [Enders and Su, 2007], [Morselli et al., 2007] and methods for key player identification [Sparrow, 1991], [Borgatti, 2003]. Network oriented research in this domain is ordinarily done by either assuming a fixed network topology or by the use of empirical historical data [Magouirk et al., 2008], [Asal et al., 2007]. However, data on covert networks is often inaccurate and anecdotal due to the widespread secrecy surrounding governmental data-sets. Mathematical models provide an alternative method for gaining insight into covert organizational structures. Once the data becomes available these models can be evaluated and adjusted if necessary.

For many types of (overt) networks the position of their connection topology between the extremes of order and randomness has been established [Watts, 1998], [Watts,

2004]. However, little is known about the exact position of the connection topology of covert networks, and consequently about their resilience against disruption. The current chapter, based on Lindelauf et al. [2011], shows where covert networks are positioned by making use of their topological characterization as secrecy influenced communication structures introduced in chapters 3 and 4. We find that the common characterization of social systems as small-world networks is generally not applicable to covert networks. This phenomenon can be explained by the fundamental dilemma such organizations have to solve: how to efficiently coordinate and exercise control while at the same time remaining secret. We corroborate our results with empirical findings of the active core of a heroin distribution network in New York City [Natarajan, 2006] and Jemaah Islamiyah's bombing of a Bali nightclub [Koschade, 2006]. In addition we show that a covert network topology is strongly resilient against disruption strategies focused on capturing and isolating highly connected individuals, partly explaining the difficulties in disrupting transnational criminal and terrorist networks.

It has been known for some time that covert networks have to deal with problems as coordination, secrecy, loyalty and trust. In our analysis thus far we focused on coordination and secrecy because recent theoretical results and empirical investigations stress the importance for criminal as well as terrorist organizations to make a trade-off between efficient coordination and control on the one hand and maintaining secrecy on the other [Morselli et al., 2007]. Even though criminal and terrorist groups differ in the sense that criminal objectives often involve monetary profit whereas terrorist objectives are ideological, security is an important concern for any covert organization. We argued in the preceding chapters that the underlying mechanism to many covert operations is the networked topology: information is exchanged on communication networks, weapons, drugs and humans diffuse through trafficking networks and loose syndicates of entrepreneurs meet in affiliation networks. It is therefore of paramount importance to understand these network structures.

In chapter 3 we introduced a multi-objective optimization framework to analyze the structure of covert networks taking the secrecy versus information tradeoff into account. That this tradeoff exists is intuitively clear: if everybody in the covert organization knows everybody else, then the security risk to the organization is very high because the exposure of an individual potentially exposes the entire organization. On the other hand, a very sparsely connected organizational network topology is difficult to coordinate and control, simply because efficient communication between individuals in such an organization is hard. We captured these critical considerations by use of an information measure I, a

secrecy measure S, and a balanced trade-off measure μ, see chapter 3 and 4.

Covert networks evolve, i.e., organized crime is increasingly operating in fluid network structures rather than more formal hierarchies and 'it would be naive to think that terrorists and their networks would remain invariant to measures designed to track and infiltrate the inner workings of their organizations' [Enders and Su, 2007]. To what kind of structures do these criminal and terrorist networks evolve? Clearly, we argue that the proactive counterterrorism activities after 9/11 have resulted in terrorist networks adopting more decentralized, non-hierarchical networks, i.e., they have taken secrecy explicitly into account as design parameter. Similarly Mexican drug cartels have become more decentralized due to more stringent law enforcement activities. Thus these covert networks are a very special subset of general social networks about which a great deal is known [Wasserman and Faust, 1994]. For instance it is well known that many social networks can be characterized as small-worlds , i.e., most individuals in the network can be reached by a small number of steps. The evidence concerning terrorist network structures however is often anecdotal, providing an impetus for the development of theoretical models of covert networks. The aim of this chapter is therefore to analyze the structure of secrecy influenced covert networks, investigate their small-world properties and the resulting consequences on their survivability properties. The important insight is that covert networks do not appear to be small-worlds, a fact that can be motivated from a secrecy standpoint. In addition we will present some empirical proof of this claim. Next we investigate the resilience of these covert network structures against disruption. We find that covert network structures perform well against disruption; actually they outperform common social networks in case of targeted attacks.

6.2 Small-world network analysis

As before a covert network is modeled by a graph $g = (N, E)$, where N represents the set of members (criminals, terrorists or cells) of the organization and E represents the links among these members. For instance such links may represent the exchange of drugs or the communication over the internet.

For $g \in \mathbb{G}(n, m)$ the characteristic path length is defined by

$$L(g) = \frac{1}{2}\frac{T(g)}{n(n-1)} = \frac{1}{2I(g)},$$

the definition the total distance $T(g)$ and the information measure $I(g)$ can be found in

chapter 3. The definition of the clustering coefficient is given by [Watts, 1998],

$$C(g) = \frac{1}{n}\sum_{i\in N} C_i,$$

where

$$C_i = \begin{cases} \frac{|N_i(g)|}{|\Gamma_i(g)|(|\Gamma_i(g)|-1)} & \text{if } |\Gamma_i(g)| \geq 2 \\ 0 & \text{otherwise.} \end{cases}$$

Here $\Gamma_i(g) = \{j \in N | l_{ij}(g) = 1\}$ is the set of neighbors of node i in network g, and $N_i(g) = \{\{k,l\} \in \Gamma_i(g) | l_{kl}(g) = 1\}$ is the set of neighbor pairs of node i that are connected in g [Strogatz, 2001]. Small-world networks are characterized by low L and high C. When compared to random networks a small-world network satisfies $L \approx L_{random}$ and C is of a different order of magnitude than C_{random}.

We use the same information measure of a graph $g \in \mathbb{G}(n,m)$ as defined in chapter 3, i.e.,

$$I(g) = \frac{n(n-1)}{T(g)}.$$

We adopt the secrecy measure from Section 3.5, scenario 3. That is let $g \in \mathbb{G}(n,m)$ then

$$S(g) = \frac{2m(n-2) + n(n-1) - \sum_{i\in N} d_i^2(g)}{(2m+n)n}$$

and set

$$\mu(g) = S(g)I(g) = \frac{(n-1)(2m(n-2) + n(n-1) - \sum_{i\in N} d_i^2(g))}{(2m+n)T(g)}.$$

Strogatz [2001] quantified small-worlds as networks with low characteristic path length L and high clustering coefficient C relative to random networks with the same number of nodes. The characteristic path length L is a global indicator that measures the typical separation between two individuals in the network. Obviously the characteristic path length L will be inversely related to the information measure I. This is because a high separation between the terrorists in the network will make it difficult for them to coordinate and control as reflected by a low information measure. The clustering coefficient C, a local indicator, measures the cliquishness of a typical neighborhood. In many social networks an individual's friends are also friends among each other. Clearly, in covert networks this in general will not be the case because too many interconnections among individuals will degrade the secrecy of such an organization. The clustering coefficient C is based on the number of edges that exist between the neighbors of each node.

It is generally argued that covert organizations facing an exogenous threat transform into hybrid network structures that lie somewhere in between sparse networks (such as the star, ring, lattice or path) and the complete network (all-to-all communication) in which everybody is connected to everybody else [Arquilla and Ronfeldt, 2001]. To simulate this transformation we interpolate between star, ring, path or lattice networks and the complete network and for each instance establish the optimality of the resulting network with regard to the secrecy versus information tradeoff characterization. To investigate whether the small-world characterization of various social networks also holds true for covert networks, we thus generate intermediate hybrid networks. Our procedure starts with an initial network (a star, ring, path or lattice) and with a probability p that each non-existing edge is added. For fixed values of p, corresponding to intermediate networks, several indicators relating to the small-world structure (L, C) and the secrecy versus information tradeoff (μ) of the network are computed and averaged over 20 realizations. In Figure 6.1 we plot the normalized values of L, C and μ versus p starting from each of the four possible initial networks. It can be seen that the maximum value of μ, indicating approximate optimal covert network structures, is typically not attained at low characteristic path lengths and high clustering coefficients, features that characterize small-world networks. For instance, if the initial graph equals the path graph (Figure 6.1 top right), then it can be seen that μ attains its maximum around $p = 0.09$, where the value of L is small and C does not attain a high value. In particular, the tiny fraction of shortcuts that suffices to create small-worlds, although increasing the ability to communicate, increases the security risk to a covert network. Clearly covert networks favor low clustering because this is in the interest of secrecy whereas low characteristic path lengths ensure the necessary communication and control abilities. Our simulation shows that the small-world phenomenon is not characteristic of theoretically optimal covert networks.

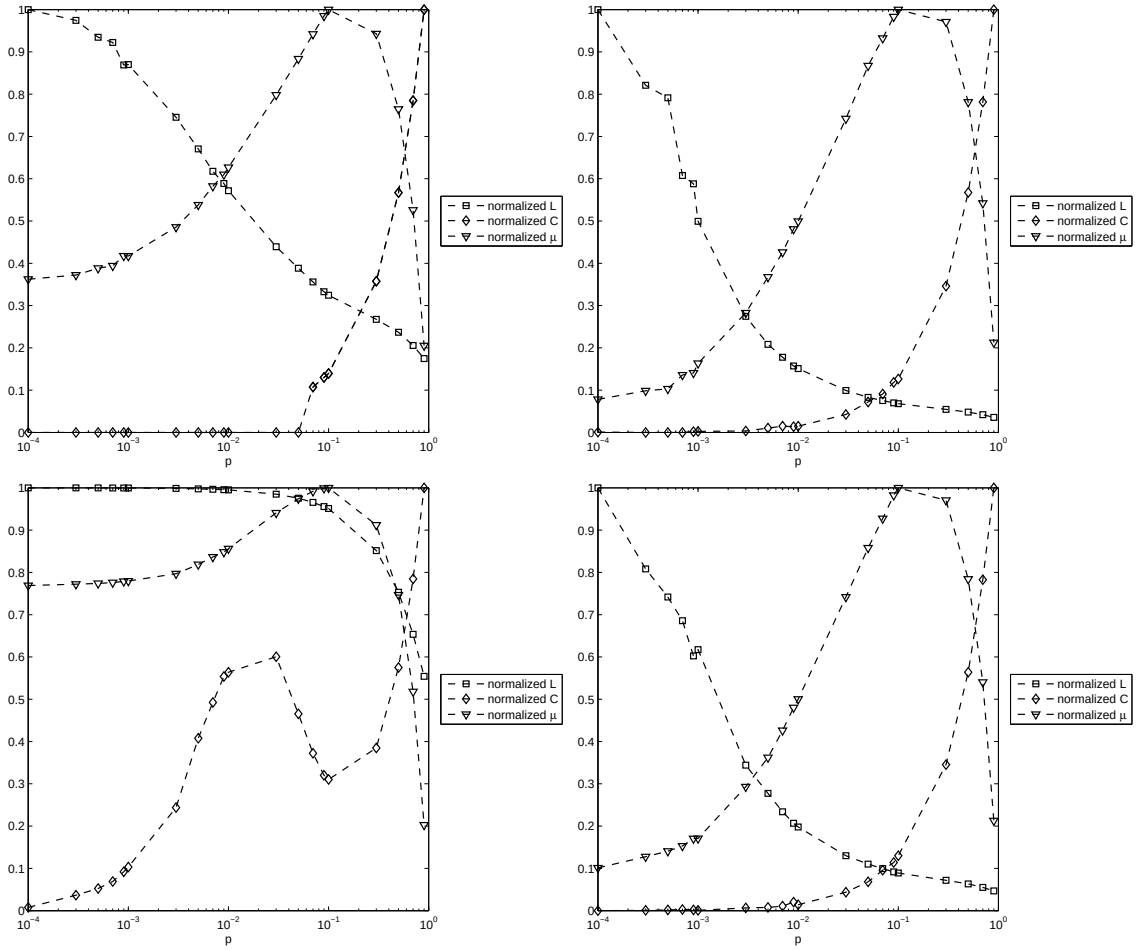


Figure 6.1: Normalized characteristic path length L, clustering coefficient C and performance measure μ as a function of the probability p with which each vacant edge is added to an initial network which is a lattice (top left), path (top right), star (bottom left) or ring (bottom right). All networks have 100 nodes and L, C and μ are averaged over 20 realizations for each of the values for p.

6.3 Empirical examples

We compute the characteristic path length and the clustering coefficient for two real covert networks: a heroïn distribution network in New York city and the Jemaah Islamiyah cell responsible for the Bali bombings in 2002. More information (i.e., network size, density, nature of interaction) on both examples can be found in Natarajan [2006] and Koschade [2006]. Here we only consider the network structure, i.e., the nodes and the links among the nodes. We compare the values of their characteristic path length and the clustering

coefficient of a graph with the same number of nodes in which every possible edge occurs independently with probability $p = \frac{1}{2}$, i.e., a random graph. To compare these outcomes with networks that are small-worlds we present an empirical example of a film-actor network [Watts, 1998] . It can be seen that both empirical covert networks do not show the small-world phenomenon because their characteristic path lengths as well as clustering coefficients are comparable to those of a random network (Table 6.1). The film actor network however is a small-world: its characteristic path length is of similar order as the random graph on the same number of nodes whereas its clustering is much higher.

	L_{actual}	L_{random}	C_{actual}	C_{random}
Heroin Network	4.74	4.93	0.44	0.13
Jemaah Islamiyah	3.18	3.11	0.89	0.46
Film actors	3.65	2.99	0.79	0.00027

Table 6.1: Comparison of characteristic path lengths and clustering coefficients of two empirical covert networks and an overt empirical network and 100.000 randomly generated graphs with the same number of nodes.

It is also interesting to investigate whether these empirical covert networks optimize their structure according to the theoretical framework on the secrecy versus information tradeoff dilemma. Therefore we compute μ for both empirical covert networks (μ_{he} and μ_{ji} respectively) and we approximate the optimal value of μ on networks of the same order (μ_{he}^{opt} and μ_{ji}^{opt} respectively). We find that $\frac{\mu_{he}}{\mu_{he}^{opt}} = \frac{0.33}{0.39} = 0.85$ and that $\frac{\mu_{ji}}{\mu_{ji}^{opt}} = \frac{0.28}{0.38} = 0.74$. We may conclude that both networks attain empirical values for μ that are close to optimal and hence correspond to the region (Figure 6.1) within which the existence of a possible small-world structure is contradicted. Thus we obtain further evidence for the fact that covert organizations are not small-worlds. In the next section we will explain the advantage of adopting structures differing from small-worlds.

6.4 Covert network resilience

Generally speaking, in countering a covert network, the capture or isolation of individuals is a key strategy, the effect of which is in part determined by the network's robustness properties. For instance a common strategy in the war on drugs in Mexico is to use elite police units to target the drug trade's kingpins , i.e., the key leaders. Another example is the U.S. government's strategy on decapitating Al Qaeda by pursuing high-value

targets. In complex network theory it has been shown that networks with a few highly connected nodes (hubs) are resistant to random failures because these hubs dominate their topology [Albert and Barabasi, 2000]. However, this comes at the cost of vulnerability to deliberate attacks on such hubs. This appears one of the reasons why empirical covert organizations, instead of relying on a few hubs, have evolved into decentralized, non-hierarchical structures as theoretically quantified by our secrecy versus information trade-off performance measure. A case in point is the Gulf's cartel 2007 evolution into a decentralized structure which has made it more resilient to concerted attacks by rival cartels and Mexican security forces. Another example is Al Qaeda's [Sageman, 2004, 2008] structure that among others appears to consist of local groups that self-organize by radicalization and interconnect for instance through the internet. There is no top to bottom leadership or organization. What results is a sparsely connected network safeguarding secrecy, however with low separation (due to the internet's global reach). To understand the resilience of such organizational forms we investigate the effect of the removal of a fraction of nodes of an approximate optimal covert network on the basis of the secrecy versus information performance measure.

A theoretically optimal covert network was approximated on $n = 100$ individuals as follows. We let $p \in \{0.3, 0.4, 0.5, 0.6, 0.7\}$ and for each fixed p we generated 100.000 random graphs with each possible edge present independently and identically distributed with probability p. Among these 500.000 networks the one that attained the highest value for μ was selected. Next we compare two scenarios: a fraction f of nodes is either removed randomly from such an approximate optimal covert network or the same fraction f being removed consists of nodes with the highest degrees. Results are plotted in Figure 6.2 (left) in case of random removal and in Figure 6.2 (right) in case of targeted removal.

From Figure 6.2 (left) it can be seen that the fraction of randomly removed nodes does not seem to affect the performance of the remaining network structure very much, i.e., μ is only slightly decreasing with increasing values of f. Only after a very large fraction of nodes has been removed ($f \approx 0.75$) does an effect take shape, which can be explained by the disintegration of the network.

Figure 6.2 (right) on the targeted removal of high degree nodes shows a surprising result. Even though the information measure decreases rapidly with increasing f, the total performance measure μ increases with respect to the fraction f of targeted removals. Thus the more one focuses a destabilization strategy on the targeted removal of central individuals the more a covert organization's capacity to coordinate and control is reduced

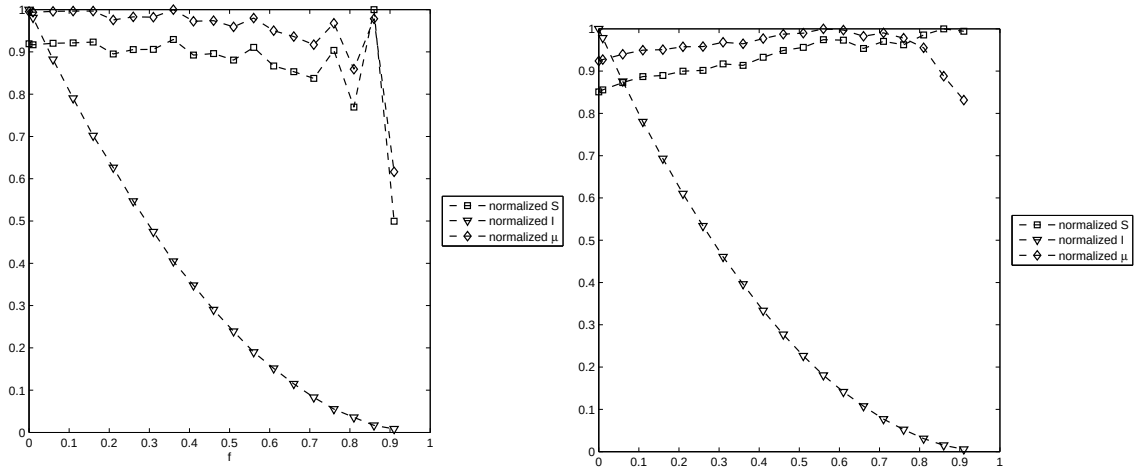


Figure 6.2: Normalized values of S, I and μ as function of the fraction f of randomly (left) and targeted (right) removed nodes.

but the higher its performance in balancing the information versus secrecy trade-off will be. Only at very high values for the fraction $f \approx 0.8$ does the performance measure start to decrease. The implication for covert networks is obvious. Their evolution towards global, sparsely connected, leaderless networks has enabled them to survive the continuing targeted attack on their nodes.

6.5 Remarks and observations

Modeling the fact that covert organizations are aware of their need to balance secrecy and information, our analysis shows that their network topology will not satisfy a 'small-world' characterization as common in many social systems. In addition we presented empirical evidence to support this claim. That criminal and terrorist networks avoid small-world structures can be explained by the low secrecy a highly clustered networked organizational form offers. Another reason for adopting a non small-world topology is found in the remarkable advantage the derived network topology offers against targeted removal. It is known that overt network topologies will show fast degradation in case of removal of hubs [Albert and Barabasi, 2000]. However we have shown that covert networks adopting secrecy and information balanced networks are perfectly capable to outlast targeted attacks. This may partly explain why current transnational criminal and terrorist networks appear to be so resilient: as long as disruption strategies do not completely disintegrate the network such efforts only strengthen their ability to attain a

balance at remaining secret while being operationally effective, instead of disabling them to operate at all.

Chapter 7

Centrality in covert networks

'The really Happy person is one
who can enjoy the scenery when on a detour'
- Anonymous

7.1 Introduction

In chapters 3 to 6 we analyzed covert networks from a design perspective. In those chapters we developed models of covert networks and analyzed various theoretical aspects such as optimal network structures with respect to the secrecy versus information bargaining trade-off, the location of risky interactions and the resulting resilience consequences of network structures that are close to optimal. In this chapter we will take a different view on covert networks. That is, instead of considering design issues by taking the position of the covert organization, we now switch to the opposite viewpoint. We consider the situation where one is confronted with a dataset of (covert) networks and one wants to find or identify those individuals that are important, have power or are central in some sense. Often these datasets are of a heterogenous nature. They not only contain information about who communicates with whom, but generally all kind of other information such as duration, frequency and time of communication, geographical locations, type of flow (money, gossip, e-mail, drug packages), affiliations and personal details (age, nationality, religion, political affiliation, education, etc.). Especially since the birth of modern day computing, increasing computational power and storage capacity have all contributed to the rapid growth of datamining in counterterrorism applications. It is apparent that a need exists for such applications. Some of the ideas in this chapter are based on Lindelauf and Blankers [2010].

Network science has a lot to offer in identifying key players engaged in networks. Graph theory develops models of networks and studies their properties in general. The combination of graph theory with sociology culminates in social network analysis that among others focuses on the identification of the 'most important' actors in a social network [Wasserman and Faust, 1994]. However it should be recognized that almost all graph theoretic centrality measures focus on the network *structure*, whereas in reality the available data contains much more information. Precisely because of this heterogeneity of data a need exists for centrality models that can incorporate such variety in their analysis. Game theory can help in developing rankings of players based on such extra information. Remember that cooperative game theory studies situations in which players can generate benefits by working together. Clearly covert organizations consist of players working together to achieve a goal. A typical example is a group of insurgents trying to carry out attacks with improvised explosive devices. To successfully launch such an attack several tasks have to be conducted, i.e., finances have to be arranged, the bomb material has to be acquired, the bomb has to be built and reconnaissance has to be conducted at the potential attack site, etc. Covert groups rely on communication networks to do such acts of recruitment and planning [Tsvetovat and Carley, 2005]. Therefore it is not only interesting to investigate how these players can operate in an optimal way, but also how power is allocated among them. Game theoretic centrality, also known as *power indices*, can be used to study such rankings of players in a network [Jackson, 2008], [Amer and Giminez, 2004], [Gomez et al., 2003]. Since cooperative game theory assigns a value to each possible coalition of players it becomes possible to not only model the structure of the network among the players in a coalition but also additional information that is available about such a coalition can be taken into account.

Rankings of players in covert networks, based on either graph theory or game theory, can aid the decision maker in identifying central players in covert networks. Such rankings can be used to allocate observation resources and to formulate destabilization strategies such as determining which players should be isolated from the network. In this chapter we will describe the application of cooperative game theory to the determination of key players in covert organizations. In Section 7.2 we will discuss the concept of centrality, both from a graph theoretic and game theoretic viewpoint. We will apply these ideas to two case studies of covert networks, being Jemaah Islamiyah's Bali attack in Section 7.3 and Al Qaeda's 9/11 attack in Section 7.4.

7.2 Centrality in networks

It is no exaggeration to state that centrality is one of the most studied concepts in sociology. Starting in the 1970's numerous measures have been proposed to quantify this concept, both from a graph theoretic and a sociological perspective [Brandes and Erlebach , Eds.], [Breiger, 2004], [Freeman, 2005], [Beauchamp, 1965], [Bonacich, 1987]. The combination of graph theory with sociology culminated in social network analysis [Wasserman and Faust, 1994], [Scott, 2000], [Wellman and Berkowitz, 1988], [Stephenson and Zelen, 1989]. For a good overview of graph theory for instance see Bollobas [Bollobas, 1998], [Bollobas, 1986] .

Borgatti and Everett [2006] introduced a categorization of centrality measures by matching them to the kinds of flows that they are appropriate for. This because often these measures make implicit assumptions about the manner in which traffic flows through a network. More specifically they defined a typology of centrality measures based on the kind of trajectories that traffic may follow (geodesics, paths, trails or walks) and the method of spread (broadcast, serial replication or transfer). It was found that centrality measures can be regarded as generating expected values for certain kinds of node outcomes given implicit models of how traffic flows. The most popular standard centrality measures are degree , betweenness and closeness and they will be discussed in the next sections.

7.2.1 Standard centrality

As already mentioned the three most well-known centrality measures are *degree*, *betweenness* and *closeness* centrality. These measures are implemented in software that is used in law enforcement and intelligence applications worldwide. We will therefore introduce and discuss them here.

Degree centrality measures the number of direct relations a player holds in the network. The normalized degree centrality $C^g_{degree}(i)$ of player i in graph $g = (N, E)$ is defined by

$$C^g_{degree}(i) = \frac{d_i(g)}{|N| - 1}.$$

The idea behind the use of degree as a measure of centrality clearly is that the more people one knows the more important one is. However, importance not only depends on

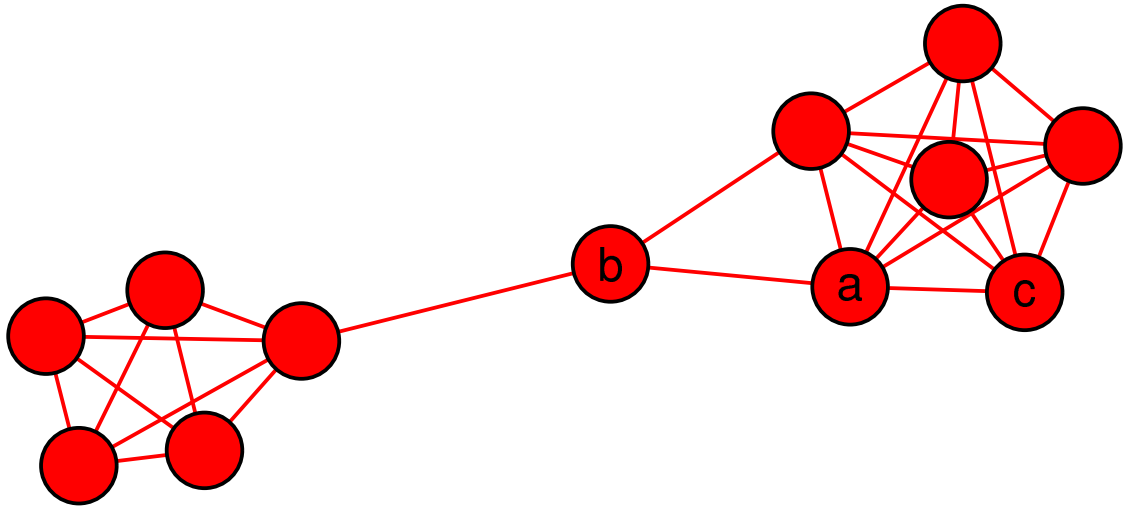


Figure 7.1: Simple of network consisting of two clusters.

the number of individuals one knows in a network, but also on their structural position in the network. Consider Figure 7.1.

Clearly the player denoted with 'b' has a lower degree centrality than player 'c'. However intuitively he plays a more important role in the network. The concept of betweenness centrality quantifies this intuition.

Betweenness centrality, first introduced by Freeman, measures how many shortest paths pass through a given vertex [Freeman, 1977]. Let $g = (N, E)$ and denote the number of shortest paths between player i and j by g_{ij}. In addition let g_{ikj} be the number of shortest paths between player i and j that pass through player k. The normalized betweenness centrality measure is then defined by

$$C^g_{betw}(k) = \frac{2}{(|N|-1)(|N|-2)} \cdot \sum_{\substack{i,j \in N \\ i<j \\ i,j \neq k}} \frac{g_{ikj}}{g_{ij}}.$$

Again consider Figure 7.1. The degree centrality of player b equals $C^g_{degree}(b) = 0,2727$, and the degree of player a equals $C^g_{degree}(a) = 0,5455$. However note that if players in the left cluster want to communicate with players in the right cluster they should communicate (in)directly via player b. It follows that $C^g_{betw}(a) = 0,2182$ and $C^g_{betw}(b) = 0,5455$. In addition it can be seen that players only connected to players in the left or right clusters score a betweenness centrality value of 0, i.e., $C^g_{betw}(c) = 0$. Note that $C^g_{degree}(c) = 0,4545$. Thus even though player c knows many people he is not

Player	Degree	Betweenness	Closeness
a	$0,5455$	$0,2182$	$0,5500$
b	$0,2727$	$0,5455$	$0,5789$
c	$0,4545$	0	$0,4231$

Table 7.1: Standard centrality values corresponding to Figure 6.1.

a so-called *gatekeeper* in the sense that he connects different clusters. It follows that different centrality measures yield different rankings of individuals. Not surprisingly this is due to the difference in context that respective centrality measures try to capture.

Finally the normalized closeness centrality of player i is defined by

$$C^g_{close}(i) = \frac{|N| - 1}{\sum_{j \in N} l_{ij}(g)}.$$

Closeness centrality quantifies the distance a player in the network has to all other players in the network. Borgatti argues that the essence of closeness is time-until-arrival of entities that flow through the network [Borgatti and Everett, 2006]. This in contradistinction to betweenness centrality which measures the frequency-of-arrival of flow in a network.

We summarize the standard centrality values corresponding to Figure 7.1 in Table 7.1. In addition we present the resulting ranking based on these values in Table 7.2. Note that these centrality measures only consider the network *structure*, and do not take additional information into account. This motivates the need for game theoretic power indices that are able to take additional information into account.

Degree	Betweenness	Closeness
a	b	b
c	a	a
b	c	c

Table 7.2: Ranking of players in figure 7.1.

Note that according to all three standard centrality measures player a is more important than player c. However the relation between other player pairs is inconclusive and depends on the measure used.

7.2.2 Game theoretic centrality

It was already noted that cooperative game theory comprises many different models among which *transferable utility games* are by far the most common [Neumann and Morgenstern, 1944]. One can think of a TU game as an allocation problem in which players can form coalitions, and each coalition gets some total payoff upon cooperation. Such models can also be used to analyze the concept of centrality, [Grofman and Owen, 1982], [Owen, 1986]. Myerson was the first to model *restricted* cooperation by means of an undirected graph [Myerson, 1977] and characterized a corresponding allocation rule which represented the 'power' of players in that specific cooperative game. Subsequently Myerson [1980] and Borm et al. [1992] provided alternative characterizations and allocation rules. Gomez et al. [2003] introduced a family of centrality measures based on this characteristic function approach.

The power of using centrality measures based on cooperative game theory is the fact that it enables the incorporation of much more than network *structure* alone into the analysis. Thus additional information, such as properties of the individuals as well as their collectives (money flows, who attended which meeting, participation in illegal activities, signs of radicalization, etc.) can be taken into account. Therefore we argue that game theoretic centrality measures, or *power indices* as they are commonly called, are useful in the analysis of covert networks. This is done by choosing the appropriate characteristic function corresponding to the context under consideration. One of the most common power indices, the Shapley value, is used as power index to determine the importance of the players, i.e., to set up a ranking based on all the available information.

More formally for a finite set N we denote the collection of all its subsets by 2^N. An element of R^N is denoted by a vector $x = (x_i)_{i \in N}$. An ordering of the elements in N is a bijection $\sigma : \{1, ..., |N|\} \to N$, where $\sigma(i)$ denotes which element in N is at position i. The set of all $|N|!$ orderings of N is denoted by $\Pi(N)$. Remember that a *TU game* is a pair (N, v), where $N = \{1, ..., n\}$ denotes the set of players and $v : 2^N \to R$ is the *characteristic function*, assigning to every coalition $S \subset N$ of players a value $v(S)$. By convention $v(\emptyset) = 0$. We denote the class of all TU games with player set N by TU^N. The *marginal vector* $m^\sigma(v)$ of a game $v \in TU^N$ corresponding to the ordering $\sigma \in \Pi(N)$ is defined by

$$m^\sigma_{\sigma(k)}(v) = v(\{\sigma(1), ..., \sigma(k)\}) - v(\{\sigma(1), ..., \sigma(k-1)\})$$

for all $k \in \{1, ..., n\}$.

To 'measure' the importance of player i in the different coalitions $S \subset N$ with $i \in S$, we look at his *marginal contributions* , i.e., $v(S) - v(S \setminus \{i\})$.

Denote the *Shapley value* of game $v \in TU^N$ [Shapley, 1953] by $\Phi(v)$. It is defined as the average of the marginal vectors

$$\Phi(v) = \frac{1}{n!} \sum_{\sigma \in \Pi(N)} m^\sigma(v). \tag{7.1}$$

An alternative expression of the Shapley value is

$$\phi_i(v) = \sum_{S \subset N, i \notin S} \frac{|S|!(|N| - 1 - |S|)!}{|N|!}[v(S \cup \{i\}) - v(S)] \quad \text{for all } i \in N. \tag{7.2}$$

In the next subsection we first introduce characteristic functions of games that represent the network structure, those games are known as connectivity games. Next we will show how additional information can be taken into account (in addition to network structure) by developing what are called weighted connectivity games. Both case studies in the coming sections are analyzed using standard centrality measures and case specific weighted connectivity measures to incorporate the additional information that is available in each specific context.

Connectivity games

We are interested in the centrality of players in a network and it thus seems obvious to adopt a game v that reflects the structural position of players in covert networks. A *connectivity* game associated to graph $g \in G^n$ is defined by Amer and Giminez [2004]

$$v_g^{conn}(S) = \begin{cases} 1 & \text{if } S \subset N \text{ is connected by } g \text{ and } |S| > 1 \\ 0 & \text{otherwise} \end{cases} \tag{7.3}$$

Thus a coalition $S \subset N$, restricted to a communication graph g, attains a value $v_g^{conn}(S) = 1$ if the players in that coalition can communicate, and $v_g^{conn}(S) = 0$ otherwise.

Connectivity centrality now is defined by the Shapley value of this game, i.e.,

$$C_{conn}^g(i) = \phi_i(v_g^{conn}).$$

To illustrate connecitivity game centrality consider the following two examples.

Example 7.1:
Assume an intelligence agency holds information on a certain individual which we will call a. He is suspected of being an accomplice to a terrorist act. Analysis of communication data reveals that a communicated with b, c and d. In addition it is revealed that b and d are known to have communicated with each other. We denote the resulting network with $g = (N, E)$, i.e., $N = \{a, b, c, d\}$ and $E = \{ab, ac, ad, bd\}$. The resulting network structure is presented in Figure 7.2.

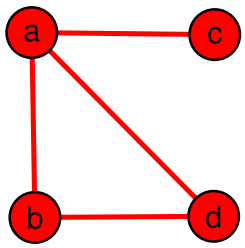


Figure 7.2: Example of four player network.

We present the characteristic function of the corresponding connectivity game v_g^{conn} in Table 7.3.

S	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{a,b\}$	$\{a,c\}$	$\{a,d\}$	$\{b,c\}$
$v_g^{conn}(S)$	0	0	0	0	1	1	1	0

S	$\{b,d\}$	$\{c,d\}$	$\{a,b,c\}$	$\{a,b,d\}$	$\{a,c,d\}$	$\{b,c,d\}$	$\{a,b,c,d\}$
$v_g^{conn}(S)$	1	0	1	1	1	0	1

Table 7.3: Characteristic function corresponding to Example 7.1.

We compute the corresponding Shapley value C_{conn}^g and present it in Table 7.4 together with the values of the three standard centrality measures.

Player	Connectivity	Degree	Betweenness	Closeness
a	0,6667	1	0,6667	1
b	0,1667	0,6667	0	0,7500
c	0	0,3333	0	0,6000
d	0,1667	0,6667	0	0,7500

Table 7.4: Centrality values of connectivity and standard centrality measures.

In Table 7.5 we present a ranking based on each of the four centrality measures. If players attain equal values they are given an asterisk($*$).

Connectivity	Degree	Betweenness	Closeness
a	a	a	a
b^*	b^*	b^*	b^*
d^*	d^*	d^*	d^*
c	c	c^*	c

Table 7.5: Ranking of players in Example 7.1.

It can be seen that $C^g_{conn}(a) > C^g_{conn}(b)$, $C^g_{conn}(b) = C^g_{conn}(d)$ and that $C^g_{conn}(c)$ attains the lowest value. Both the standard centrality measures as well as connectivity centrality denote player a as being the most important. The ordering of the players generated by connectivity centrality equals that of degree and closeness centrality. It is interesting to note that betweenness centrality is very coarse grained, i.e., players b, c and d all attain a betweenness score of 0. ◇

Example 7.2:

In Figure 7.3 another network is shown to illustrate the various centrality measures. Due to symmetry of the network we can distinguish 5 different persons within the network. These persons are denoted by the letters A to E. It can be seen that the network consists of two clusters. Person C and D function as *gatekeepers* between these clusters.

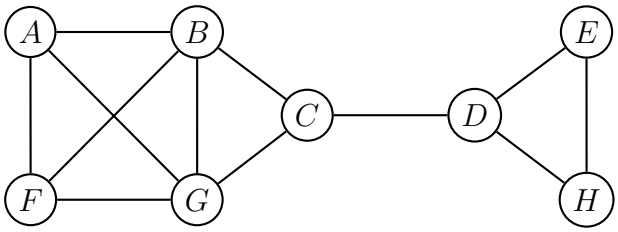


Figure 7.3: Example of a network with two clusters.

The following rankings are obtained when the standard and game theoretic centrality measures are applied to the network in Figure 7.3.

Degree	Betweenness	Closeness	Connectivity
b	c	c	c
a^*	d	b	d
c^*	b	d	e
d^*	a^*	a	b
e	e^*	e	a

Table 7.6: Ranking of persons a-e in Figure 7.3 with respect to standard and game theoretic centrality.

7.3 Case 1: Jemaah Islamiyah in Bali

On October12 2002 one of the deadliest attacks in Indonesia's history occurred on the island of Bali. In total 202 innocent civilians died as a result of this attack. After a long trial a number of members of the violent extremist group Jemaah Islamiyah were found guilty of planning and perpetrating this attack.

Jemaah Islamiyah (JI) was officially founded in 1993 in Maleysia. Its goal became the founding of an Islamic state in Indonesia [Wise, 2005]. The spiritual leaders of JI were Abdullah Sungkar and Abu Bakar Bashir. JI is partioned into four territorial divisions (*mantiqis*) corresponding to the peninsulas of Maleysia and Singapore; Java; Mindanao, Sabah, and Sulawesi; and Australia and Papua. During the eighties the founders and leaders of Jemaah Islamiyah fought on the side of the *mujahideen* against the Russians in Afghanistan. During the nineties terrorist training camps were founded in the Philippines [Council on Foreign Relations, 2009]. A little later it became apparent that Jemaah Islamiyah engaged in relations with Al Qa'ida. During this period JI received financial as well as material support, and in addition it is known that several members of Jemaah Islamiyah trained in Afghan training camps [International Crisis Group, 2002]. A good example of the intimate relation between Al Qa'ida and Jemaah Islamiyah is the close connection between Mohammed Atef, Khalid Sheikh Mohammed and Riduan Isamuddin (military leader of Jemaah Islamiyah, also known as Hambali). They agreed that Jemaah Islamiyah would conduct reconnaissance of potential targets and prepare the necessary logistics in the area of operation. Al Qa'ida would then support such operations with bomb making expertise and suicide attackers [Kean et al., 2002]. Another well known example of close cooperation between JI and Al Qa'ida is the Kuala Lumpur meeting in 2000, organized by Hambali. Some reports indicate that both the attack on the USS Cole as well as 9/11 were planned during that meeting [Rollins, 2010]. The close collaboration

with Al Qa'ida caused Jemaah Islamiyah to develop into a pan-Asiatic network stretching from Maleysia and Japan in the north, to Australia in the south [Gunaratna, 2003], [Abuza, 2003]. In 1998 Jemaah Islamiyah started the so-called *uhud* project. The aim of this project was to remove Christians as well as Hindus from regions in Indonesia, such that pure Islamic enclaves could be founded that were guided by Sharia-law [Abuza, 2003]. In addition Jemaah Islamiyah started a series of attacks in 2000. The 2002 Bali attack being its most prominent one.

The Indonesian government reacted with fierce countermeasures. Over 450 members of Jemaah Islamiyah have been arrested during the last couple of years and around 250 terrorists have been persecuted [Abuza, 2003]. The spiritual leader of JI, Abu Bakar Bashir, was arrested after the attacks in Bali. However in 2006 he was released from prison again. The most important explosives expert, Muhammad Noordin Top, was killed in 2009 by Indonesian authorities. Several other prominent leaders, among others Isamuddin, Abu Dujana and Zarkasih, were also arrested. In March of 2010 Dulmatin, who was assumed to be connected to the Bali attacks in Bali, was killed during a counterterrorism raid.

7.3.1 The Bali attack

The tactical operation in Bali was conducted by Jemaah Islamiyah's Indonesian cell, headed by Hambali. A suicide terrorist detonated a vest in Paddy's bar. This caused many people to flood to the streets. A second explosion followed, caused by a so-called 'vehicle born improvised explosive' (VBIED) , a L300 van filled with about 1000 kilograms of TNT and ammonium nitrate. This resulted in the death of 202 people. Figure 7.4 shows the operational network of the Bali attack, taken from Koschade [2006]. The operational cell conducting the attack consisted of three teams, as can be seen in Figure 7.4. A team of bomb builders (green), a support team (red) and a team responsible for coordinating the attack (blue). The team of bomb builders consisted of Patek, Imron, Azahari, Dulmatin, Ghoni, Sarijo and later on Feri was added to this team. The team responsible for the support of the operation (team Lima) was made up out of Octavia, Junaedi, Hidayat, Rauf and Arnasan. The remaining players tasked with coordinating the attack were Samudra, Idris, Muklas, Amrozi and Mubarok.

7.3.2 Centrality analysis

In this paragraph we study Jemaah Islamiyah's operational network using both standard as well as weighted connectivity centrality measures.

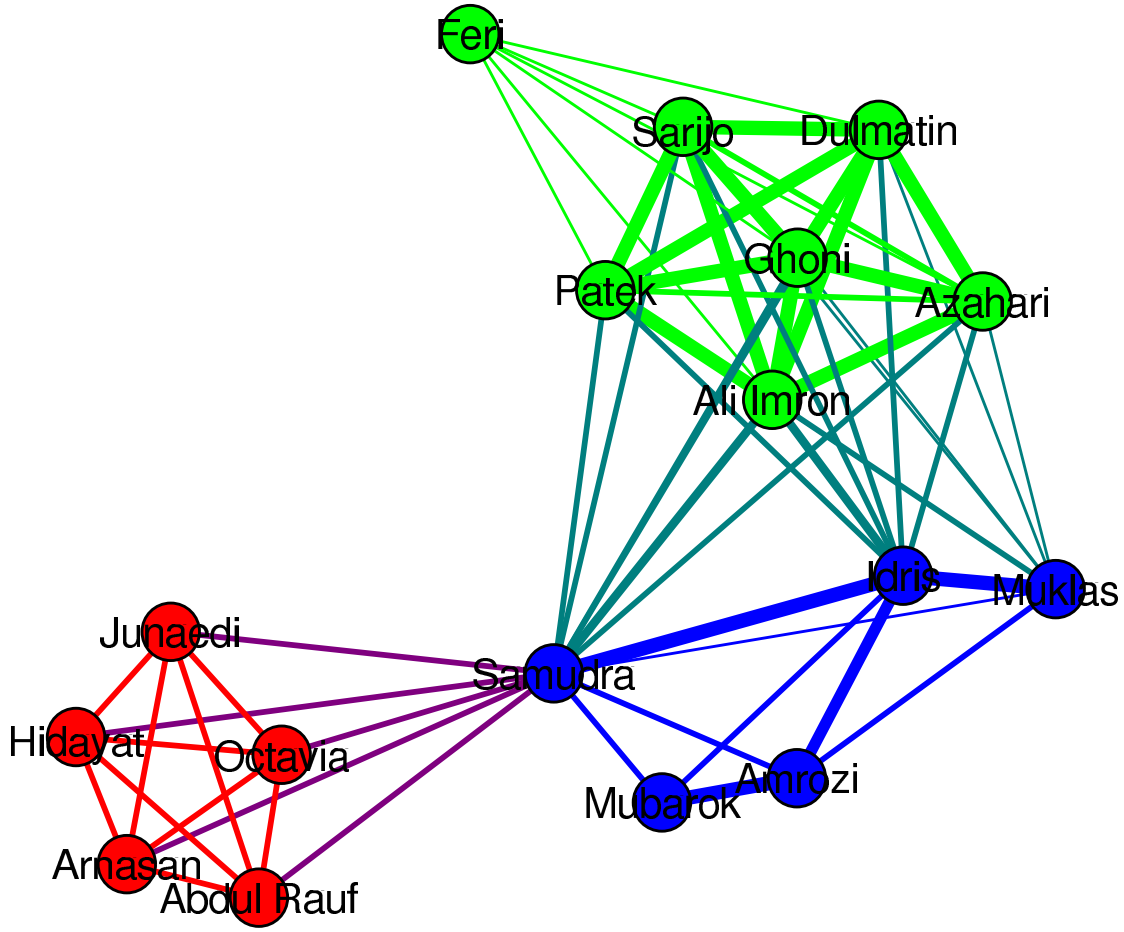


Figure 7.4: Operational network of Jemaah Islamiyah's Bali operation. Bomb building team (green), support team (red) and coordination team (blue).

Standard centrality

An analysis of the standard centrality measures degree, betweenness and closeness applied to Jemaah Islamiyah's operational network is available from the scientific literature [Koschade, 2006]. Koschade's analysis focuses on the structure of the network, i.e., he only analyzes whether a relationship exists between players in the network. Additionally he weighs the relations by analyzing the frequency and duration of each relationship. This is done by coding the interaction between cell members using the criteria 'transactional content' and 'frequency and duration of interaction', resulting in a weighted matrix with weights between 0 and 5. A weight of 0 is interpreted as there not being any relation, a weight of 5 meaning that there is highly frequent interaction of long duration. In Figure 7.4 these weights are visualized by the size of the lines connecting the players,

the bigger the size the higher the weight of that respective relationship. Koschade analyzes the network by using degree, betweenness and closeness centrality [Koschade, 2006]. Therefore he only analyzes the network structurally, he does not take into account the additional weighting of the relationships between the players in the network. We present the results of the standard centrality analysis in Table 7.7. Note that the players are ordered according to degree centrality.

Player	Degree	Betweenness	Closeness
Samudra	0,9375	0,5097	0,9411
Idris	0,6250	0,0513	0,7272
Muklas	0,5625	0,0194	0,6956
Ali Imron	0,5625	0,0139	0,6956
Dulmatin	0,5625	0,0139	0,6956
Azahari	0,5625	0,0139	0,6956
Patek	0,5625	0,0139	0,6956
Ghoni	0,5625	0,0139	0,6956
Sarijo	0,5625	0,0139	0,6956
Feri	0,3750	0	0,4849
Arnasan	0,3125	0	0,5714
Junaedi	0,3125	0	0,5714
Abdul Rauf	0,3125	0	0,5714
Octavia	0,3125	0	0,5714
Hidayat	0,3125	0	0,5714
Amrozi	0,2500	0,0028	0,5517
Mubarok	0,1875	0	0,5333

Table 7.7: Standard centrality values of players participating in Jemaah Islamiyah's Bali attack.

All three standard centrality analysis point to Samudra as being the most central player. He was envisaged as the brain' behind the operation. In addition Idris scores second most central on all three standard centrality measures. He was also known to be an important player in planning and executing the attack. Also note that the degree and closeness centrality measure do not distinguish between Muklas, Imron, Dulmatin, Azahari, Patek, Ghoni and Sarijo. This also holds, except in the case of Idris, for the betweenness centrality measure. We argue that this is due to the fact that these centrality measures only consider the network structure. We will show that using weighted connectivity centrality based on game theory allows for making more distinction between players in a network simply because it enables more information to be taken into account in the mathematical model.

Game theoretic centrality

In this paragraph we analyze Jemaah Islamiyah's Bali operational network using (weighted) connectivity centrality. The additional information that Koschade [2006] introduced regarding duration and frequency of interaction can be used in a weighted connectivity centrality analysis. In general a definition of the characteristic function should be done together with a domain expert.

We motivate our choice of characteristic function corresponding to this case study as follows. A covert organization will try to shield its important players by keeping the frequency and duration of their interaction with others to a minimum. However, to be able to coordinate and control an important player needs to maintain relationships within the network. The 'worth' of a coalition is therefore defined by the total number of binary relations that exist within that coalition divided by the sum of the weights (representing frequency and duration of interaction) on those links. Formally let $g = (N, E)$ with weights f_{ij} for all $ij \in E$ and define the characteristic function by

$$v_g^{wconn}(S) = \begin{cases} \frac{\sum_{i,j \in S, ij \in E} I_{ij}(E)}{\sum_{i,j \in S, ij \in E} f_{ij}} & \text{if } S_g \text{ is connected,} \\ 0 & \text{else.} \end{cases}$$

Note that $I_{ij} = 1$ if $ij \in E$ or else $I_{ij} = 0$.

Additionally note that if $f_{ij} = 1$ for all $ij \in E$ this definition equals the definition of connectivity centrality. It can thus be seen that the weighted connectivity centrality not only takes the structure of the network into account but it also models additional information that is available. Clearly, the choice of characteristic function always depends on the data that is available and the context of the problem. The (publicly) data available on the Jemaah Islamiyah Bali casus consists of relationships and their weighings, and the operational context consists of a cell during the planning and execution phase.

We present the results of the game theoretic centrality analysis in Table 7.8. Note that the players are ordered according to connectivity centrality.It follows from Table 7.8 that the game theoretic centrality measures are less coarse grained than the standard centrality measures. To clarify this we provide a ranking of the players for each of the five centrality measures in Table 7.9. Players that attain the same centrality value within a ranking are given a similar symbol (either $*$ or a $\bullet$). In a similar way as with standard centrality Imron, Dulmatin, Azahari, Patek, Ghoni and Sarijo attain similar centrality values. Muklas however does not. It appears that if in addition to network structure other information is taken into account (weights on edges) then the granularity of the

Speler	Connectivity	Weighted connectivity
Samudra	0,8713	0,3615
Idris	0,0494	0,0001
Muklas	0,0361	0,0481
Ali Imron	0,0340	-0,0177
Dulmatin	0,0340	0,0007
Azahari	0,0340	0,0117
Patek	0,0340	0,0039
Ghoni	0,0340	-0,0042
Sarijo	0,0340	0,0087
Feri	-0,0012	0,0319
Amrozi	-0,0042	-0,0110
Mubarok	-0,0175	-0,0130
Arnasan	-0,0275	-0,0073
Junaedi	-0,0275	-0,0073
Abdul Rauf	-0,0275	-0,0073
Octavia	-0,0275	-0,0073
Hidayat	-0,0275	-0,0073

Table 7.8: Game theoretic centrality values of Jemaah Islamiyah's Bali attack.

results increases. This granularity is even larger for weighted connectivity in comparison to (normal) connectivity. No of the players in Dulmatin's team (Imron - Sarijo) attain the same centrality value. If in practice one would have limited capacity to conduct observation such a weighted connectivity centrality analysis would yield useful results in the optimal allocation of resources.

Discussion

We compare the game theoretic centrality measures with the standard centrality measures and discuss the top 5 players. We only discuss the top 5 because we assume that in practice only limited capacity for observation is present. In addition such a centrality analysis can function as a decision support tool to optimally allocate limited resources. We present the top 5 players in Table 7.9 for each centrality measure. Note that there can be more than 5 players per ranking because sometimes players attain equal values.

First we conclude that Samudra was the most important player in this operation. He attains the highest value for all five centrality measures. This is in concordance with a ruling by judge Sudewi[1]

[1]Last retrieved May 2011 from www.nzherald.co.nz, Court sentences second man to death for Bali

Degree	Betweenness	Closeness	Connectivity	Weighted Connectivity
Samudra	Samudra	Samudra	Samudra	Samudra
Idris	Idris	Idris	Idris	Muklas
Muklas*	Muklas	Muklas*	Muklas	Feri
Ali Imron*	Ali Imron*	Ali Imron*	Ali Imron*	Azahari
Dulmatin*	Dulmatin*	Dulmatin*	Dulmatin*	Sarijo
Azahari*	Azahari*	Azahari*	Azahari*	Patek
Patek*	Patek*	Patek*	Patek*	Dulmatin
Ghoni*	Ghoni*	Ghoni*	Ghoni*	Idris
Sarijo*	Sarijo*	Sarijo*	Sarijo*	Ghoni
Feri	Amrozi	Arnasan•	Feri	Octavia*
Arnasan•	Feri•	Junaedi•	Amrozi	Abdul Rauf*
Junaedi•	Arnasan•	Abdul Rauf•	Mubarok	Hidayat*
Abdul Rauf•	Junaedi•	Octavia•	Arnasan•	Arnasan*
Octavia•	Abdul Rauf•	Hidayat•	Junaedi•	Junaedi*
Hidayat•	Octavia•	Amrozi	Abdul Rauf•	Amrozi
Amrozi	Hidayat•	Mubarok	Octavia•	Mubarok
Mubarok	Mubarok•	Feri	Hidayat•	Ali Imron

Table 7.9: Centrality ranking of players in Jemaah Islamiyah's Bali attack.

"Judge Isa Sudewi told the court today the prosecution had proven Samudra, an engineering graduate, played a key role in the bombings. 'The defendant worked behind the scenes as the coordinator so the panel of judges has an opinion that the defendant is the intellectual actor behind the bomb explosions,' she said."

In addition it can be seen that if only network *structure* is taken into account, the ranking of the 5 most important players is ambiguous. For instance, looking at degree and closeness centrality, it can be seen that players 3 (Muklas) up to 9 (Sarijo) all attain equal values. If only a total of 5 players could be observed then, using these centrality measures as ranking of importance, it is not clear which 5 players should be observed. If we look at the betweenness centrality and connectivity centrality scores we see that players 4 (Ali Imron) up to 9 (Sarijo) score similar values. In that case it thus also holds that the centrality measures are coarse and it is not possible to uniquely determine the top 5 players. However, if we look at the 5 highest ranking players in case of weighted connectivity centrality, it follows that the top 5 players can be determined unambiguously. Additionally we observe that, in comparison with the other centrality measures, the weighted connectivity centrality measure has three different players present among

bombings.

the 5 highest ranking ones. Weighted connectivity centrality assign Feri, Azahari and Sarijo among the top 5 highest ranking members instead of Idris, Imron and Dulmatin. It can thus be seen that, if additional information is added to the network structure, possibly other players make up the top highest ranking members, and that the capacity to distinguish between importance of players is increased.

On October 10^{th}, two days prior to the attack, Feri arrived. He was recruited to be the suicide bomber of Paddy's bar. The results of the centrality analysis show that Idris attains low values for all standard centrality measures. Betweenness and closeness centrality even rank him the lowest (see Table 7.9). However, weighted connectivity centrality assigns Feri as being one of the 3 most important players. It is known that Feri conducted an important task during the Bali bombings. Another player that attains a high weighted connectivity centrality value is Azahari (he attained low values on the standard centrality measures). Azahari was Jemaah Islamiyah's bomb expert and the 'brain' behind the Bali operation [Council on Foreign Relations, 2009]. If Azahari's role would have been detected or recognized in time the feasibility of the operation would have been seriously hampered.

7.3.3 Findings

Both standard as well as game theoretic centrality measures consider Samudra, Muklas, Azahari and Sarijo to be high ranking players. Samudra appears to be the highest ranking member according to all centrality measures. Weigthed connectivity centrality considers Feri to be one of the 3 highest ranking members and does not consider Idris and Ali Imron to be of much prominence with regard to the other centrality measures. Regarding the other players in the network it can be seen that their ranking is more or less the same across different centrality measures.

Without Samudra the secrecy of the network would drastically increase. Clearly this can be explained by observing the structure of the network. (Figure 7.4). From a secrecy viewpoint a network consisting of two clusters is more secret than if the clusters would have been linked: exposure of an individual in one cluster can never lead to exposure of an individual in another cluster. Of course this also sets Samudra apart if we consider his role in information exchange. Without him communication between the team responsible for building the bomb (one cluster) and team Lima (another cluster) would not have been possible. This finding reinforces Koschade's remark [Koschade, 2006]:

"The third finding is that Samudra was the weakest point in the cell, and his capture would possibly have led to the isolation of Team Lima (which included the suicide bomber

and contingency nodes) and the loss of the most active and centralized member of the network."

It is safe to say that Samudra's removal would have had a pronounced effect on the Bali operation. This paragraph has shown that centrality analysis support this conclusion.

Another interesting player in the Jemaah Islamiyah case study is Feri. He was recruited as suicide terrorist and was added to the network only in the final stages of the operation. In that sense he did not play an important role in the exchange of information. However, in hindsight we know that his removal would have uprooted the feasibility of the operation because of his role. Weighted connectivity centrality however does place him among the high ranking members. Thus it shows that taking additional information into account (in this case study weights on the links) that the results of an analysis can lead to other interesting conclusions.

7.4 Case 2: Al Qaeda and 9/11

Three and a half year before the infamous 9/11 attack Osama bin Laden issued a *fatwa* calling on all Muslims "to kill the Americans, both civilian and military, in every country in which it was possible to do so...".[2] Already in 1996 he issued a *declaration of jihad* against the United States.[3] During the nineties Bin Laden expressed his wish that the United States would withdraw from Saudi Arabia. He argued that the presence of American troops on the Arabian peninsula was an insult to the Islamic community.

7.4.1 The attack on september 11, 2001

During a presentation in Tora Bora, Khalid Sheikh Mohammed proposed an operation with trained pilots flying into buildings [Kean et al., 2002]. This proposal finally culminated in the 9/11 operation. Note that Khalid Sheikh Mohammed was also in contact with Hambali, Jemaah Islamiyah's Indonesian cell leader. The 'planes-operation' was further refined in the spring of 1999 by Bin Laden, Khalid Sheikh Mohammed and Mohamed Atef during a number of meetings in Kandahar [Kean et al., 2002]. Finally two seperate groups were prepared and sent to the United States to conduct the operation: one group in Hamburg consisting of Mohamed Atta, Ramzi Binalshibh[4], Marwan al Shehhi

[2]Declaration published in in Al-Quds al Arabi, February 23 1998, Londen.

[3]Declaration of Jihad Against the Americans Occupying the Land of the Two Holy Mosques, Al Islah (London), Sept. 2, 1996

[4]It turned out that Binalshibh could not obtain a visa, therefore he remained behind in Europe with a coordinating role.

and Ziad Jarrah and another group consisting of al Khalid al Mihdhar, Nawaf al Hazmi, Khallad and Abu Bara el Yemeni. On January 15 of 2000 Hazmi and Midhar arrived in the United States and in the early summer of 2000 the other group from Hamburg also arrived in the United States. On December 8 of 2000 the last of the four pilots arrived, Hani Hanjour in San Diego. During the summer and autumn of 2000 the other hijackers were selected by Bin Laden and his followers [Kean et al., 2002]. These hijackers arrivied in April of 2000 in the United States. The specific date of September 11^{th} was probably only determined somewhere in august of 2001. Several days before the actual attack the hijackers relocated to hotels closeby their specific airports and the remaining finances were transfered.

On tuesday morning (local time) September 11^{th} 2001 the world was shocked by two planes fying into the Twin Towers of the World Trade Center of New York. A third plane flew into the Pentagon and a fourth crashed somewhere in Pennsylvania. It turned out that 19 hijackers, most of whom were from Saudi Arabia, were directly responsible for the execution of the operation. The events leading up to this day have been described meticulousy in popular media and the academic literature [Kean et al., 2002].

7.4.2 Centrality analysis

To conduct a centrality analysis of the network responsible for this operation we use network data that was gathered by Krebs [2002]. Krebs obtained the data on the hijackers from open sources. It is to be expected that classified data on this operation is more detailed and thrustworthy. However, this data was not available for this case study. In paragraph 7.4.2 we illustrate how qualitative data can be transformed into quantitative network data by using the '9/11 commission report' [Kean et al., 2002] as source of additional information on hijackers. During the preperation of the 9/11-operation several meetings occurred where the hijackers coordinated and reported on the status of the preperations, an example of such a meeting is the meeting in Las Vegas [Krebs, 2002]. It is the network that was obtained by analyzing this meeting that will be used for the analysis of this case study. In Figure 7.5 we visualize the corresonding network. The colors in the Figure refer to the different flights of United Airlines (UA) and American Airlines (AA), i.e., UA-175 (green), UA-93 (purple), AA-77 (blue) and AA-11 (red).

First we analyze the network with standard centrality measures degree, betweenness and closeness.

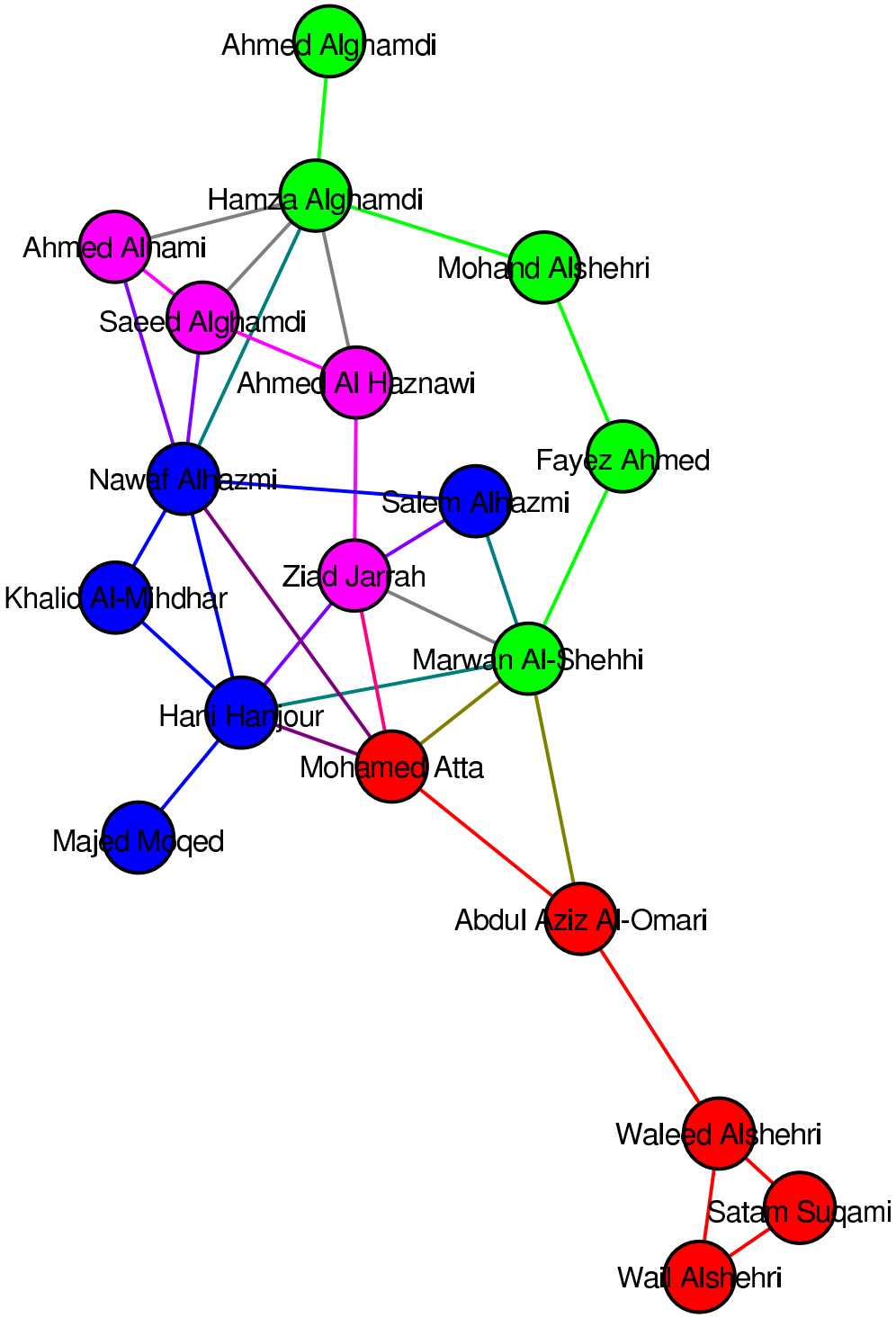


Figure 7.5: Al Qa'ida's 9/11-operational network, UA-175 (green), UA-93 (purple), AA-77 (blue) en AA-11 (red).

Standard centrality

We present the results of the standard centrality analysis in Table 7.10. The players are ordered according to degree centrality.

Player	Degree	Betweenness	Closeness
Nawaf Alhazmi	0,3889	0,3075	0,5143
Marwan Al-Shehhi	0,3333	0,2097	0,4865
Hamza Alghamdi	0,3333	0,1881	0,4390
Hani Hanjour	0,3333	0,1673	0,4865
Mohamed Atta	0,2778	0,2142	0,5143
Ziad Jarrah	0,2778	0,0751	0,4615
Saeed Alghamdi	0,2222	0,0100	0,4091
Abdul Aziz Al-Omari	0,1667	0,2941	0,4286
Waleed Alshehri	0,1667	0,2092	0,3273
Ahmed Al Haznawi	0,1667	0,0297	0,4000
Salem Alhazmi	0,1667	0,0137	0,4390
Ahmed Alnami	0,1667	0	0,3913
Mohand Alshehri	0,1111	0,0337	0,3600
Fayez Ahmed	0,1111	0,0516	0,3913
Khalid Al-Mihdhar	0,1111	0	0,3830
Satam Suqami	0,1111	0	0,2535
Wail Alshehri	0,1111	0	0,2535
Majed Moqed	0,0566	0	0,3333
Ahmed Alghamdi	0,0556	0	0,3103

Table 7.10: Standard centrality measures of Al Qa'ida's 9/11-attack.

First notice that Nawaf Alhazmi attains the highest degree and betweenness centrality score. Alhazmi was regularly in contact with Mohamed Atta during the summer of 2001. It is assumed that he conduced an important role in planning the operational part of the operation [Miller, G. and Meyer, J., 2002]. In addition it can be observed that Abdul Aziz al-Omari and Mohamed Atta attain high betweenness centrality scores. This follows from the fact that Mohamed Atta was the operational leader and Al-Omari together with Atta constituted the link between the hijackers of American Airlines flight 11 and the remainder of the network. Also note that Atta and Alhazmi attain high closeness centrality values.

Game theoretic centrality

As already noted, the power of game theoretic centrality analysis is the ability to incorporate additional information in the analysis of an operational network. Taking such additional information can be done in many ways. Remember that in the case study of Jemaah Islamiyah we used addtional information that reflected the frequency and duration of interaction between players. However a first look at the public data on Al Qaeda's 9/11 operation reveals that it only contains binary network information. However addtional reports on the 9/11-attack reveal more information on the individuals that perpetrated this attack. Using this information we will show how it can be modeled using weighted connectivity. We categorize the additional information into *player*-related information and *relationship*-related information. Clearly, the addtional information that was available in the case study of Jemaah Islamiyah consisted of relationship-related information.

Variable	**example**	**player(s)**	**weight**
Attending meetings on terror attack planning	Kuala Lumpur meeting January 2000	Nawaf al Hazmi Khalid al-Midhar	+1
Signs of radicalisation	Antisemitic and anti-American speech, talk about jihad and martyrdom, writing a will	Mohamed Atta Marwan al-Shehhi Ziad Jarrah	+1
Affiliations	Al-Quds mosque Hamburg	Mohamed Atta Ramzi Binalshibh Ziad Jarrah	+1
Accomplice to earlier attacks	Attack on USS Cole	Khalid al-Midhar	+1
Attending terror training camps	travel to Pakistan and Afghanistan	Mohamed Atta Marwan al-Shehhi Ziad Jarrah Moussaoui	+1

Table 7.11: Simple example of player-related variables.

In Table 7.11 we present an example of variables that could play a role in player-related information. In addition we indicate how such a variable can be evaluated in case of Al Qa'ida's 9/11-operation. As allready mentioned, this addtional information is obtained from the '9/11 commission report'. Note that in general a thorough analysis of historical sources will shed more light on the players that are involved in an operation. The information gathered for this case study is only used to illustrate how this can de done.

Let $g = (N, E)$ be the network and assign to every player $i \in N$ a weight w_i. Define

the characteristic function for this case by

$$v_g^{wconn}(S) = \begin{cases} \sum_{i \in S} w_i & \text{if } S_g \text{ connected,} \\ 0 & \text{else.} \end{cases}$$

We determine the weight w_i on each player i as follows. First every player in the network is given a weight of 1. Next, depending on the addtional information, the weight of player is increased depending on his score on the variables which will be defined together with analysts (see Table 7.11 for some examples). The value of a coalition then becomes the sum of the weight of its players if the underlying network is connected, otherwise the value of the coalition will be 0. Note that this definition differs from the characteristic function used in the case study of Jemaah Islamiyah.

Player	Network only	Network and addtional information
Ahmed Alghamdi	1	1
Hamza Alghamdi	1	1
Mohand Alshehri	1	1
Fayez Ahmed	1	1
Marwan Al-Shehhi	1	3
Ahmed Alnami	1	1
Saeed Alghamdi	1	1
Ahmed Al Haznawi	1	1
Ziad Jarrah	1	4
Salem Alhazmi	1	1
Nawaf Alhazmi	1	1
Khalid Al-Mihdhar	1	3
Hani Hanjour	1	1
Majed Moqed	1	1
Mohamed Atta	1	4
Abdul Aziz Al-Omari	1	1
Waleed Alshehri	1	1
Satam Suqami	1	1
Wail Alshehri	1	1

Table 7.12: Player weights in 9/11 case study.

If we take Table 7.11 as reference to determine the total weight on each player in the 9/11-case study, then the total weight of each player is given in Table 7.12.

The value of the coaltion consisting of Mohamed Atta, Marwan al-Shehhi and Abdul Aziz Al-Omari equals $3 + 4 + 1 = 8$, note that this coalition is connected in the network

(see Figure 7.5). The value of the coalition consisting of Mohamed Atta, Marwan Al-Shehhi and Satam Suqami however equals 0. This because not all players in this coalition can communicate, i.e., their network structure is not connected. We calculate the value for each coalition and use it to determine the values of weighted connectivity centrality. Note again that the weights as presented in Table 7.12 are used to illustrate how certain factors can be incorporated in a game theoretic centrality analysis.

We present the results of the game theoretic centrality analysis of Al Qaeda's 9/11 operation in Table 7.13. The players are ordered according to connectivity centrality.

Player	Connectivity	Weighted connectivity
Abdul Aziz Al-Omari	0,2366	6,0957
Hamza Alghamdi	0,2344	5,5770
Hani Hanjour	0,2234	5,4026
Waleed Alshehri	0,2034	5,5622
Marwan Al-Shehhi	0,0934	2,2026
Nawaf Alhazmi	0,0864	1,5696
Mohamed Atta	0,0476	1,6003
Ziad Jarrah	0,0323	1,3108
Ahmed Al Haznawi	0,0150	0,4966
Mohand Alshehri	0,0138	0,6300
Salem Alhazmi	0,0060	0,2804
Saeed Alghamdi	0,0053	0,2336
Fayez Ahmed	-0,0024	0,2920
Ahmed Alnami	-0,0038	0,1496
Khalid Al-Mihdhar	-0,0088	0,5612
Satam Suqami	-0,0424	-0,3690
Wail Alshehri	-0,0424	-0,3690
Ahmed Alghamdi	-0,0449	-0,5351
Majed Moqed	-0,0530	-0,6911

Table 7.13: Game theoretic centrality analysis of Al Qa'ida's 9/11 attack.

It can be seen that the game theoretic centrality values are less coarse grained than the results of the standard centrality analysis (see Tables 7.10 en 7.13). Only Satam Suqami and Wail Alshehri attain similar values for all centrality measures. If we look at Figure 7.5 it follows that both these players are exchangeable in the network, only looking at network structure.

In Table 7.14 we present a ranking of the players for each one of the centrality measures. We grouped the players, for each centrality measure, such that the players that

Degree	Betweenness	Closeness	Connectivity	W. connectivity
N. Alhazmi	N. Alhazmi	N. Alhazmi*	A. Aziz al-Omari	A. Aziz al-Omari
M. al-Shehhi*	A. Aziz al-Omari	M. Atta*	H. Alghamdi	H. Alghamdi
H. Alghamdi*	M. Atta	M. al-Shehhi$^{\bullet}$	H. Hanjour	Wd. Alshehri
H. Hanjour*	M. al-Shehhi	H. Hanjour$^{\bullet}$	Wd. Alshehri	H. Hanjour
M. Atta$^{\bullet}$	Wd. Alshehri	Z. Jarrah	M. al-Shehhi	M. al-Shehhi
Z. Jarrah$^{\bullet}$	H. Alghamdi	H. Alghamdi$^{\diamond}$	N. Alhazmi	M. Atta
S. Alghamdi	H. Hanjour	S. Alhazmi$^{\diamond}$	M. Atta	N. Alhazmi
A. Aziz al-Omari$^{\diamond}$	Z. Jarrah	A. Aziz al-Omari	Z. Jarrah	Z. Jarrah
Wd. Alshehri$^{\diamond}$	F. Ahmed	S. Alghamdi	A. al Haznawi	M. Alshehri
A. al Haznawi$^{\diamond}$	M. Alshehri	A. al Haznawi	M. Alshehri	K. al-Midhar
S. Alhazmi$^{\diamond}$	A. Al Haznawi	F. Ahmed*	S. Alhazmi	A. al Haznawi
A. Alnami$^{\diamond}$	S. Alhazmi	A. Alnami*	S. Alghamdi	F. Ahmed
F. Ahmed*	S. Alghamdi*	K. al-Midhar	F. Ahmed	S. Alhazmi
M. Alshehri*	A. Alnami*	M. Alshehri	A. Alnami	S. Alghamdi
K. al-Midhar*	K. al-Midhar*	M. Moqed	K. al-Midhar	A. Alnami
S. Suqami*	S. Suqami*	Wd. Alshehri	S. Suqami*	S. Suqami*
W. Alshehri*	W. Alshehri*	A. Alghamdi	W. Alshehri*	W. Alshehri*
A. Alghamdi$^{\circ}$	A. Alghamdi*	W. Alshehri$^{\circ}$	A. Alghamdi	A. Alghamdi
M. Moqed$^{\circ}$	M. Moqed*	S. Suqami$^{\circ}$	M. Moqed	M. Moqed

Table 7.14: Ranking of players of Al Qa'ida's 9/11-attack.

attain the same value are given the same symbol ($*$, $\bullet$, $\diamond$, $\star$ or $\circ$). Note that the degree and closeness centrality measure are coarse grained: their ranking consist of many players that attain similar values. The betweenness centrality measure is unambiguous for players that attain a positive value. Players in the periphery of the network however attain similar values.

Discussion

As was the case for the Jemaah Islamiyah case study we again discuss the 5 highest ranking players for both the standard centrality measures as well as the game theoretic centrality measures. We present these 5 hightest ranking players in Table 7.14, a line demarcating the five highest ranking players from the other ones. Note that the 5 highest ranking players according to degree and closeness actually consist of more than 5 players. Clearly this is due to the fact that certain players attain a similar centrality score for that specific centrality measure.

We observe that there is a difference between the results of the standard centrality measures and the game theoretic centrality measurs. According to the standard centrality measures Nawaf Alhazmi is the most important player in this operation. He attains the highest score for all three standard centrality measures. Additionally it can be seen that

Mohamed Atta, Marwan al-Shehhi and Abdul Aziz al-Omari are ranked among the 5 highest ranking members in case of degree, betweenness and closeness centrality. However an unambiguous ranking of these three players is impossible to construct according to one of these standard centrality measures. The game theoretic centrality measures consider Abdul Aziz al-Omari to be the most important player. The remaining players among the 5 highest ranking ones are Hamza Alghamdi, Marwan al-Shehhi, Hani Hanjour and Waleed Alshehri. Note that Nawaf Alhazmi does not occur in both game theoretic rankings among the 5 highest ranking players. If we take a closer look at Figure 7.5 it appears that this is due to the fact that there are other players that form bridges in the network. One of these players for instance is Hamza Alghamdi, together with Marwan al-Shehhi he links United Airlines flight 175 with the remaining hijackers. Additionally it can be seen that Abdul Aziz al-Omari and Waleed Alshehri are essential in linking American Airlines flight 11 to the remainder of the network. Therefore these players appear to attain high values according to the game theoretic centrality measures.

In addition it can be seen that even connectivity centrality, in comparison to the standard centrality measures, results in a different ranking of the players. Weighted connectivity does not yield any new insights however. This may be due to the fact that the additional information that is used in this case study is only marginal.

7.4.3 Findings

Standard centrality measures determine Nawaf Alhazmi as being the most important player for the 9/11 planes-operation. The destabilizing effect after the removal of Nawaf Alhazmi however is only minor. Abdul Aziz al-Omari forms a bridge between two parts of the network. Because betweenness centrality designates him as being the second important player, his removal together with that of Nawaf Alhazmi would result in mission degredation. If however we would use degree or closeness centrality in a destabilization effort, then more than two players need to be removed from the network to halt the operation. Weighted connectivity centrality however seems more useful in determing the crucial links in the network. Removal of the most important player according to weighted connectivity centrality, Abdul Aziz al-Omari, directly results in network destabiliztion and hence mission degredation. We conclude that (weighted) connectivity centrality is most useful in determing which players to remove from the network in this case study.

7.5 Remarks and observations

By introducing solution concepts from cooperative game theory and combining them with graph theory it becomes possible to define centrality measures that more closely reflect covert groups organized according to networked topologies. For instance in case of drug trafficking, values for coalitions can represent the amount of money that respective coalitions obtain by cooperating. A subsequent analysis of their network structure by the application of (weighted) connectivity games can help to determine key players in such structures. Here we showed how the cooperative game theoretic solution concept known as the Shapley value, combined with (weighted) connectivity games, can aid in refining centrality measures for covert networks. We analyzed several standard network topologies and presented an example on weighted connectivity games. We illustrated the results of these concepts by two case studies: Jemaah Islamiyah's Bali attack and Al Qaeda's 9/11 operation.

Future research should focus on the application of the proposed game theoretic centrality measures to real terrorist networks and the development of specific cooperative games to model the corresponding situations. In addition algorithms for efficiently computing the Shapley value of a weighted connectivity game should be developed.

Chapter 8

Covert projects and related games

'We, and all others who believe in freedom as deeply as we do, would rather die on our feet than live on our knees.'
- Franklin D. Roosevelt

8.1 Introduction

Various groups, networks, organizations and even state-actors conduct covert operations that can be viewed as projects consisting of tasks. Think of the (covert) development of nuclear weapons by states, the development and implementation of improvised explosive devices by insurgents or terrorists, and the acquisition, manufacturing and movement of synthetic drugs by criminals. Even though such projects are highly dissimilar, there is a commonality underlying them all: they consist of tasks that have to be conducted by players. For instance, to conduct an attack with an improvised explosive device finances have to be arranged, players need to be recruited and the operation has to be planned. Furthermore bombs have to be built, stored and moved to a target location that has to be reconnoitered. Finally the bombs have to be installed and (possibly) remotely detonated. Clearly these tasks are not conducted by a single player, or even a single group of players. On the contrary, often such operations are conducted by groups that form opportunity coalitions and loose affiliations [Swanson, 2007]. In a similar way the synthetic drug trade can be viewed as a project consisting of the acquisition of precursor chemicals and equipment, the manufacturing of the drug, the disposal of waste material and the movement and selling of the drugs. Again such a project can be viewed as tasks conducted by different players [Huisman and Smits, 2008].

To interdict covert projects the international community and governmental agencies have several means at their disposal. Within the law enforcement domain the kingpin

strategy is commonly used to disrupt criminal organizations. For instance on December 3 1999, the U.S. President signed into law the Foreign Narcotics Kingpin Designation Act blocking all property and interests in property, subject to U.S. jurisdiction, owned or controlled by significant foreign narcotics traffickers (Foreign Narcotics Kingpin Designation Act (21 U.S.C. '1901-1908, 8 U.S.C. '1182)). Within the counterterrorism domain a similar strategy, by the name of key-leader engagement, is employed [Jordan, 2009]. Both consist of attempts at disrupting enemy operations by identifying and isolating key players of the opposing party. To determine which players are important many qualitative and quantitative techniques have been developed [Carley, 2006]. Most quantitative techniques focus on the social relationships that exist among the criminals or terrorists, i.e., they rely on centrality measures developed in social network analysis [Koschade, 2006]. Though important, such methodology usually neglects the nature of the project that the opposing organization is trying to conduct.

Projects on the other hand have been studied abundantly from several different perspectives. For instance Bergantinos and Sanchez [2002a] analyze projects in which the time needed to execute tasks is estimated and the planned duration of a project can be determined. Due to a delay or the expedition of such projects extra costs or rewards may arise. Branzei et al. [2002] and more recently Estevez-Fernandez et al. [2007] study such problems from a game theoretic perspective. Game theory has also been applied to the study of Project Evaluation and Review Technique (PERT) whose main purpose it is to compute the minimum time needed in order to complete all tasks of a project, see for instance Bergantinos and Sanchez [2002b]. Researchers in the counterterrorism and security domain study effective methods of hindering the completion of projects, such as Reed [2004] and more recently Brown's study of resource-limited interdiction actions that maximally delay completion time of a proliferator's weapons project [Brown et al., 2009].

In this chapter we are interested in the same question that invokes the use of social network analysis in key leader engagement which we studied in chapter 7: 'which players are important?'. However we analyze this question from the vantage point of players that are participants in covert projects. Generally much less is known about the details of the tasks in a covert project (like a terrorist attack or human trafficking) than in an overt one. For instance, the duration of certain tasks is generally not known. Therefore we model a *covert* project simply as a set of tasks. We know however that those tasks have to be enabled by individuals. We assume that governmental and intelligence agencies confronted with covert projects have the means at their disposal to discover which

individuals enable what tasks. What remains is to determine which of the players to focus on. Clearly, a player that has a monopoly on the completion of a certain task is important with respect to the completion of the project. For instance consider a situation where there is only one player who enables the smuggling of precursor material needed to manufacture amphetamine in a certain geographical region. Without such a player the executability of the synthetic drugs project in that region is essentially hampered. In reality however there might be more players capable of enabling a task. Hence it becomes imperative to be able to evaluate the importance of players engaged in such projects by taking the possible structure among the players and the tasks into account. We introduce the so-called project enabling task structure to model the relation between the players and the tasks. Our assumption is that if a player enables a certain task in a project, then he can only do this in a single project at some fixed time. For instance if a player enables the smuggling of precursor material in a synthetic drug project at a certain moment he can not facilitate the smuggling of precursor material in another project at the same time. We impose no restrictions on the projects in which a player enables *different* tasks. Thus it could very well be that a player enables the smuggling of precursor material in one synthetic drug project and at the same time he enables the financing of a synthetic drug in another project. Hence it is possible that a group of players can enable more than one project at the same time.

To measure the power of players in a project enabling task structure we introduce and characterize the project power measure. The analysis of a project enabling task structure by use of the project power measure essentially yields a partition of the set of players into core leaders, peripheral leaders and inessential players. A player is called inessential if without him the total number of projects that is enabled does not change. Core leaders are those players that can enable a project alone or with inessential players only. The remaining players are the peripheral leaders. Without a peripheral leader one less project is enabled, however a peripheral leader can not enable a single project with inessential players only. Next we associate to each project enabling task structure a project game. We prove that the compromise value of this game equals the project power measure. We investigate the core of this game and provide a condition such that the core equals the convex hull of all so-called critical task group vectors.

The remainder of this chapter is organized as follows: in Section 8.2 we define projects and introduce project enabling task sets. Section 8.3 introduces and characterizes the project power measure. In Section 8.4 we introduce associated project games and in particular we show that the corresponding compromise value equals the project power

measure. Finally we analyze the structure of the core of project games.

8.2 Covert projects

In this section we will formally define project enabling task structures. Loosely speaking a project consists of tasks and there are players, each one capable to execute a certain subset of tasks. This does not mean that a player actually conducts that task, only that through his coordinating role he acts as an enabler of that task in the project. We assume that a player can not enable the same task in two projects simultaneously. Consider the following illustrating example.

Example 8.1:
An Improvised Explosive Device (IED) cell consisting of 21 members is tasked with attacking allied troops. A typical 'IED-project' together with the tasks that players enable is given in Table 8.1 below.

Task	Task group
1: recruitment and planning	$\{1, 2, 20, 21\}$
2: logistical sources identification	$\{3, 4, 5, 6, 16, 21\}$
3: IED building and training	$\{1, 11, 13, 15, 21\}$
4: IED storage	$\{1, 11, 20, 21\}$
5: reconnaissance and preparation of attack site	$\{1, 13, 20, 21\}$
6: movement of IED	$\{2, 4, 9, 10, 12, 14, 18, 21\}$
7: placement of IED	$\{1, 15, 20, 21\}$
8: attack	$\{7, 8, 10, 17, 19, 21\}$

Table 8.1: Example of IED-project and tasks that players enable.

Clearly the players involved in this project comprise the set $N = \{1, ..., 21\}$. A set of players that can enable a task in the IED-project is called a task-group, and the set of task groups is called a project enabling task structure. In this example the project enabling task structure equals

$$\begin{aligned}\mathbb{T} \;=\; &\{\{1, 2, 20, 21\}, \{3, 4, 5, 6, 16, 21\}, \{1, 11, 13, 15, 21\}, \{1, 11, 20, 21\},\\ &\{1, 13, 20, 21\}, \{2, 4, 9, 10, 12, 14, 18, 21\}, \{1, 15, 20, 21\}, \{7, 8, 10, 17, 19, 21\}\}.\end{aligned}$$

The presence of player 2 in the task group called 'movement of IED' means that he can act as enabler of the movement of an IED from a source to a destination. The actual moving of that specific IED is not necessarily done by player 2 himself, but through his influence

he can guarantee that the IED will be moved. Moreover we assume that the IED-cell as a whole can conduct four IED-projects since players enable tasks simultaneously, and a task can be enabled in a single project only. For instance player 21 will enable IED storage in a single IED project only. As there are just four players that enable the task of IED storage there can never be more than four simultaneous projects. In addition it can be seen that without player 21 only a total of three simultaneous IED-projects can be conducted. Without player 3 however, who only enables the task of logistical sources identification, the number of projects that the IED-cell can conduct remains unchanged. Note that we do not require that a player enables all his tasks in the same project. For instance it can be seen that player 1,4,7 and 21 enable a total of two projects. This could be realized by having player 21 enable all tasks in a single project and players 1,4 and 7 enabling the tasks in the other project. But alternatively it could also mean that player 21 enables all tasks except the 'attack' in the first project and player 1,4 and 7 enabling all tasks in the second project except that player 7 enables the attack for the first project and player 21 enables the attack for the second project. It is clear that task groups that consist of a minimal number of players are critical. Note that criticality of a task group does not depend on the actual interpretation of the task (i.e., whether it is IED storage or placement of the IED for instance) but only on the *structure* of the project enabling task set. The collection of critical tasks equals

$$C(\mathbb{T}) = \{1, 4, 5, 7\}.$$

Players within a critical task group are called essential, i.e.,

$$E(\mathbb{T}) = \{1, 2, 11, 13, 15, 20, 21\}.$$

Without an essential player the number of projects that is enabled is reduced by one. Players outside $E(\mathbb{T})$ are called inessential and the set of inessential players is denoted by $I(\mathbb{T})$. Observe that if an inessential player is removed the number of projects that can be enabled does not change. Of the essential players we call player 1 and 21 core leaders, denoted by $CL(\mathbb{T}) = \{1, 21\}$, because player 21 enables all 8 tasks as previously mentioned. Player 1 does not enable task 2, 6 and 8, but is also considered to be a core leader because he can form a coalition that enables a single IED-project with inessential players only. This does not hold for the remaining essential players. Therefore they are called peripheral leaders, denoted by $PL(\mathbb{T}) = \{2, 11, 13, 15, 20\}$. ◇

Formally we define a *project* as a set $P = \{1, ..., p\}$ and call its elements *tasks*. Given a finite player set N and a project $P = \{1, ..., p\}$ we define the corresponding *project*

enabling task structure $\mathbb{T}_P^N = (T_1, ..., T_p)$ with $T_i \in 2^N$. Elements of $\mathbb{T}_P^N$ are called *task groups*. Task group $T_j \in \mathbb{T}_P^N$ corresponds to task $j \in P$. If a player belongs to T_j this is interpreted as the player being a task enabler for task $j \in P$. Without that player the number of times that the *task* $j \in P$ can be conducted is reduced by one. We will omit the subscript P and superscript N whenever the project and player set under consideration are clear from the context.

The set of all possible project enabling task structures regarding a project $P = \{1, ..., p\}$ and player set N is denoted by $PETS(N, p)$. Let PETS denote *all* project enabling task structures. An enabled project in P is an ordered sequence of players $(a_1, ..., a_p)$ such that $a_i \in T_i$ for all $i \in P$. We assume that a player can not enable a specific task in more than one enabled project simultaneously. Thus if $(a_1, ..., a_p)$ and $(b_1, ..., b_p)$ are two different enabled projects then $a_k \neq b_k$ for all $i \in P$. The total number of projects coalition N can conduct is

$$tot(\mathbb{T}) = min_{k \in \{1,...,p\}} |T_k|.$$

Let $\mathbb{T} = (T_1, ..., T_p) \in PETS(N, p)$ and $S \subset N$. We define the set of tasks that the coalition S enables by

$$G_{\mathbb{T}}(S) = \{k \in \{1, ..., p\} | T_k \cap S \neq \emptyset\}.$$

The project enabling task structure $\mathbb{T}_{-S}$ that results when the players in S are removed from all task groups is denoted by

$$\mathbb{T}_{-S} = (T_1 \setminus S, ..., T_p \setminus S).$$

A task is critical if it forms a 'bottleneck' in carrying out a project, i.e., if the size of the corresponding task group is minimal among the size of all task groups. The set $C(\mathbb{T})$ of *critical* tasks in $\mathbb{T}$ is denoted by

$$C(\mathbb{T}) = \{k \in \{1, ..., p\} || T_k| \leq |T_l| \text{ for all } l \in \{1, ..., p\}\}.$$

Observe that if $k \in C(\mathbb{T})$ then $|T_k| = tot(\mathbb{T})$.

A player is called *essential* if he is a member of at least one critical task group. The set of all essential players is denoted by $E(\mathbb{T})$. All other players are called *inessential*. The set of inessential players $I(\mathbb{T})$ is given by $I(\mathbb{T}) = N \setminus E(\mathbb{T})$. It readily follows that by removing an essential player the total number of projects that can be conducted is reduced by one, i.e.,

$$tot(\mathbb{T}_{-\{i\}}) = tot(\mathbb{T}) - 1 \quad \text{for all } i \in E(\mathbb{T}). \tag{8.1}$$

Moreover $tot(\mathbb{T}_{-\{i\}}) = tot(\mathbb{T})$ for all $i \in I(\mathbb{T})$.

Finally we partition the set of essential players into *core leaders* and *peripheral leaders*. A player $i \in E(\mathbb{T})$ is a *core leader* if

$$G_{\mathbb{T}}(\{i\}) \supset C(\mathbb{T}) \text{ and for all } k \in P \setminus G_{\mathbb{T}}(\{i\}) \text{ it holds that } I(\mathbb{T}) \cap T_k \neq \emptyset.$$

Thus a player is a core leader if either he can enable project on his own or he can enable it together with inessential players only. We denote the set of *core leaders* by $CL(\mathbb{T})$ and the set $E(\mathbb{T}) \setminus CL(\mathbb{T})$ of peripheral leaders by $PL(\mathbb{T})$.

To actually identify this partition of the set of players we present the following algorithm.

Algorithm to identify core leaders, peripheral leaders and inessential players
Input: Project enabling task set $\mathbb{T} \in PETS(N, p)$.
Initialization:
Set $z^* = min_{T_k \in \mathbb{T}} |T_k|$.
Determine the set of critical tasks $C(\mathbb{T})$, i.e, $k \in C(\mathbb{T})$ if $|T_k| = z^*$.
Iteration 1: Determine the set of inessential players.
For $i \in N$
Step 1. For each T_k, $k \in C(\mathbb{T})$, check if $i \in T_k$.
Step 2. If i in at least one critical task group then $i \notin I(\mathbb{T})$, else $i \in I(\mathbb{T})$.
End iteration 1.
Iteration 2: Determine the core leaders and the peripheral leaders.
For $i \in N \setminus I(\mathbb{T})$
Step 1. Check if i is a member of *all* the critical task groups. If not set $i \in PL(\mathbb{T})$ and go to the next player, else
Step 2. Check if for all T_k such that $k \notin C(\mathbb{T})$ and $i \notin T_k$ there is a $j \in I(\mathbb{T})$ with $j \in T_k$. If not set $i \in PL(\mathbb{T})$ and go to the next player, else
Step 3. Set $i \in CL(\mathbb{T})$.
End iteration 2.
Output: Partition of N into $CL(\mathbb{T})$, $PL(\mathbb{T})$ and $I(\mathbb{T})$.

8.3 The project power measure

In the previous section we partitioned the set of players corresponding to a project enabling task structure in core leaders, peripheral leaders and inessential players. Here

we evaluate the role of each player in contributing to the total number of simultaneous projects the players in the project enabling task structure can conduct. We do this by introducing and characterizing a power measure on the class of all project enabling task structures.

A *power measure* f assigns to each $\mathbb{T} \in PETS$ a vector $f(\mathbb{T}) \in \mathbb{R}^N$.

We introduce the project power measure. Since core leaders are those players that exactly enable *one* project with inessential players only the project power measure assigns a value of 1 to those players. Without an *inessential* player the number of projects that is enabled remains unaffected. The project power measure assigns a value of 0 to those players. The peripheral leaders are less important than the core leaders but more important than the inessential players. The project power measure divides the remainder of the total number of projects evenly among the peripheral leaders. Formally we define the project power measure θ on the class of all project enabling task structures by

$$\theta_i(\mathbb{T}) = \begin{cases} 1 & \text{if } i \in CL(\mathbb{T}) \\ \frac{tot(\mathbb{T})-|CL(\mathbb{T})|}{|PL(\mathbb{T})|} & \text{if } i \in PL(\mathbb{T}) \\ 0 & \text{else} \end{cases} \tag{8.2}$$

if $\mathbb{T} \in PETS$.

Let f be an arbitrary power measure. We introduce and discuss several properties of f that arise naturally from the interpretation of project enabling task structures. Efficiency captures the fact that the total power is equal to the total number of simultaneous projects that can be conducted.

Efficiency (EFF):
If $\mathbb{T} \in PETS(N,p)$, then $\sum_{i\in N} f_i(\mathbb{T}) = tot(\mathbb{T})$.

The power structure does not depend on the presence of core leaders.

Core Leader Removal (CLREM):
If $\mathbb{T} \in PETS(N,p)$ and $j \in CL(\mathbb{T})$ it holds that $f_i(\mathbb{T}) = f_i(\mathbb{T}_{-\{j\}})$ for all $i \in N \setminus \{j\}$.

A player whose removal does not change the total number of projects the organization can enable holds no power.

Inessential Removal (IREM):
If $\mathbb{T} \in PETS(N,p)$ and $i \in N$ is such that $tot(\mathbb{T}) = tot(\mathbb{T}_{-\{i\}})$, then $f_i(\mathbb{T}) = 0$.

With $\mathbb{T} = (T_1, T_2, ..., T_p) \in PETS(N,p)$, $i,j \in N$, define $\mathbb{T}_{i \leftrightarrow j} = (U_1, U_2, ..., U_p)$ by

$$U_k = \begin{cases} T_k \quad \text{if } i,j \in \mathbb{T} \text{ or } i,j \notin \mathbb{T} \\ T_k \setminus \{j\} \cup \{i\} \text{ if } j \in T_k, i \notin T_k \\ T_k \setminus \{i\} \cup \{j\} \text{ if } j \notin T_k, i \in T_k. \end{cases}$$

Player i and j are said to be *symmetric with respect to* $\mathbb{T}$ if $\mathbb{T} = \mathbb{T}_{i \leftrightarrow j}$.

Symmetry (SYM):
For all $\mathbb{T} \in PETS(N,p)$ with $i,j \in N$ symmetric with respect to $\mathbb{T}$ it holds that $f_i(\mathbb{T}) = f_j(\mathbb{T})$.

Next consider a project enabling task structure without core leaders. We assume that extending a project with a task group, that is of similar size to another task group and only differs by the constituency of peripheral leaders, will leave the power among the players unaltered.

Task addition (ADD):
Let $\mathbb{T} = (T_1, ..., T_p) \in PETS(N,p)$ with $CL(\mathbb{T}) = \emptyset$. Let $T_k \in \mathbb{T}$ and let $T_{p+1} \in 2^N$ be such that $T_{p+1} \cap I(\mathbb{T}) = T_k \cap I(\mathbb{T})$, $|T_{p+1}| = |T_k|$. Define $\mathbb{T}' = (T_1, ..., T_p, T_{p+1}) \in PETS(N, p+1)$. Then $f(\mathbb{T}) = f(\mathbb{T}')$.

Theorem 8.3.1 *A project power measure is equal to θ if and only if it satisfies EFF, CLREM, IREM , SYM and ADD.*

Proof:
We first show that θ satisfies EFF, CLREM, IREM, SYM and ADD:

Efficiency (EFF):
Let $\mathbb{T} \in PETS(N,p)$ then

$$\sum_{i \in N} \theta_i(\mathbb{T}) = |CL(\mathbb{T})| + |PL(\mathbb{T})| \cdot \frac{tot(\mathbb{T}) - |CL(\mathbb{T})|}{|PL(\mathbb{T})|} = tot(\mathbb{T}).$$

Core Leader Removal(CLREM):
Let $\mathbb{T} \in PETS(N,p)$ and $j \in CL(\mathbb{T})$. Clearly $I(\mathbb{T}_{-\{j\}}) = I(\mathbb{T})$. In addition it can be seen that if $i \in CL(\mathbb{T})$, $i \neq j$, then also $i \in CL(\mathbb{T}_{-\{j\}})$. Moreover it readily follows that if $k \in PL(\mathbb{T})$ then also $k \in PL(\mathbb{T}_{-\{j\}})$. Hence $\theta_i(\mathbb{T}) = \theta_i(\mathbb{T}_{-\{j\}})$ for all $i \in N \setminus \{j\}$.

Inessential Removal(IREM):
Let $\mathbb{T} \in PETS(N,p)$ and let $i \in N$ be such that $tot(\mathbb{T}) = tot(\mathbb{T}_{-\{i\}})$. Then (8.1) implies that $i \in I(\mathbb{T})$. Hence $\theta_i(\mathbb{T}) = 0$.

Symmetry (SYM):
Let $\mathbb{T} \in TS(N,p)$ and let $i,j \in N$ be such that $\mathbb{T} = \mathbb{T}_{i \leftrightarrow j}$. Then $\theta_i(\mathbb{T}) = \theta_i(\mathbb{T}_{i \leftrightarrow j}) = \theta_j(\mathbb{T})$.

Task additivity(ADD):
Let $\mathbb{T} = (T_1, ..., T_p) \in PETS(N, p)$ with $CL(\mathbb{T}) = \emptyset$. Let $i \in N$. Since $CL(\mathbb{T}) = \emptyset$ there either exists $k \in C(\mathbb{T})$ such that $k \notin G_{\mathbb{T}}(\{i\})$ or there exists $k \in P \setminus G_{\mathbb{T}}(\{i\})$ with $I(\mathbb{T}) \cap T_k = \emptyset$. In $\mathbb{T}' = (T_1, ..., T_p, T_{p+1})$ there either exists $k \in C(\mathbb{T}')$ such that $k \notin G_{\mathbb{T}'}(\{i\})$ or there exists $k \in P \setminus G_{\mathbb{T}'}(\{i\})$ with $I(\mathbb{T}') \cap T_k = \emptyset$, hence $CL(\mathbb{T}') = \emptyset$. In addition observe that for all $i \in E(\mathbb{T})$ it holds that $i \notin I(\mathbb{T}')$ since $|T_{p+1}| \geq tot(\mathbb{T})$. Moreover if $i \in I(\mathbb{T})$ then $i \notin E(\mathbb{T}')$. Hence $\theta(\mathbb{T}) = \theta(\mathbb{T}')$.

To prove the reverse let f be a power measure that satisfies EFF, CLREM, IREM, SYM and ADD. We will show that $f = \theta$.

Let $\mathbb{T} \in PETS(N, p)$ and $i \in CL(\mathbb{T})$. Then it follows that

$$f_i(\mathbb{T}) = \sum_{j \in N} f_j(\mathbb{T}) - \sum_{j \in N \setminus \{i\}} f_j(\mathbb{T}) = \sum_{j \in N} f_j(\mathbb{T}) - \sum_{j \in N \setminus \{i\}} f_j(\mathbb{T}_{-\{i\}}) = tot(\mathbb{T}) - tot(\mathbb{T}_{-\{i\}}) = 1.$$

Hence $f_i(\mathbb{T}) = 1$ for all $i \in CL(\mathbb{T})$. Note that the second equality follows from CLREM, the third equality follows from EFF and the fourth equality follows from (8.1).

If $i \in I(\mathbb{T})$, then $tot(\mathbb{T}) = tot(\mathbb{T}_{-\{i\}})$. Hence by (IREM) it follows that $f_i(\mathbb{T}) = 0$ for all $i \in I(\mathbb{T})$. It readily follows that

$$\begin{aligned} \sum_{i \in N} f_i(\mathbb{T}) = tot(\mathbb{T}) &= \sum_{i \in CL(\mathbb{T})} f_i(\mathbb{T}) + \sum_{i \in PL(\mathbb{T})} f_i(\mathbb{T}) + \sum_{i \in I(\mathbb{T})} f_i(\mathbb{T}) = \\ &= |CL(\mathbb{T})| + \sum_{i \in PL(\mathbb{T})} f_i(\mathbb{T}). \end{aligned}$$

Consequently $\sum_{i \in PL(\mathbb{T})} f_i(\mathbb{T}) = tot(\mathbb{T}) - |CL(\mathbb{T})|$.

Define $\mathbb{T}' = (U_1, U_2, ..., U_p) = \mathbb{T}_{-CL(\mathbb{T})}$. Clearly $CL(\mathbb{T}') = \emptyset$. Let $i, j \in PL(\mathbb{T})$. Clearly by CLREM it suffices to show that $f_i(\mathbb{T}') = f_j(\mathbb{T}')$. Without loss of generality let

$$p(i) = \{k \in \{1, ..., p\} | i \in U_k \text{ while there is no } l \in \{1, ..., p\} \text{ s.t. } U_l = U_k \setminus \{i\} \cup \{j\}\}$$

and

$$p(j) = \{k \in \{1, ..., p\} | j \in U_k \text{ while there is no } l \in \{1, ..., p\} \text{ s.t. } U_l = U_k \setminus \{j\} \cup \{i\}\}.$$

Define U_{p+k} by $U_{p+k} = U_l \setminus \{i\} \cup \{j\}$ for all $k \in \{1, ..., |p(i)|\}$ where l equals the k^{th} element of $p(i)$. Define $U_{p+|p(i)|+k}$ by $U_{p+|p(i)|+k} = U_l \setminus \{i\} \cup \{j\}$ for all $k \in \{1, ..., |p(j)|\}$ where l equals the k^{th} element of $p(j)$. Let$\mathbb{T}'' = (U_1, ..., U_p, U_{p+|p(i)|}, U_{p+|p(i)|+1}, U_{p+|p(i)|+|p(j)|})$, then clearly i and j are symmetric with respect to $\mathbb{T}''$ and it follows that

$$f_i(\mathbb{T}') = f_i(\mathbb{T}'') = f_j(\mathbb{T}'') = f_j(\mathbb{T}').$$

Where the first and third equality follow from repeated use of ADD and the second equality follows from SYM. □

8.4 Project games

In this section we introduce so-called project games to study project enabling task structures and the power of players that enable tasks. We analyze the compromise value, the core and the core cover of a project game and their relationship to the convex hull of critical task group vectors.

8.4.1 Compromise value

First we recall some preliminaries of cooperative game theory from chapter 2. Let N be a finite set of players and denote by 2^N the collection of all subsets of N. Elements of 2^N are called *coalitions*. A TU-game is a pair (N, v) where $v : 2^N \mapsto \mathbb{R}$ with $v(\emptyset) = 0$. The function v is called the *characteristic function* and $v(S)$ is called the *worth* or *value* of the coalition $S \subset N$. We are interested in the importance of players that arises because they enable tasks in projects. We define a transferable utility *project game* $(N, v_{\mathbb{T}})$ corresponding to project enabling task structure $\mathbb{T} = (T_1, ..., T_p) \in PETS(N, p)$ by

$$v_{\mathbb{T}}(S) = min_{k\in\{1,...,p\}}|T_k \cap S| \quad \text{for all} \quad S \subset N. \tag{8.3}$$

Thus $v_{\mathbb{T}}$ represents the number of simultaneous projects coalition S enables in project enabling task structure $\mathbb{T}$. Observe that $v_{\mathbb{T}}(N) = tot(\mathbb{T})$.

The compromise value for a game (N, v), introduced by Tijs [1981], is the efficient compromise between the utopia vector $M(v) \in \mathbb{R}^N$ and the minimum right vector $m(v) \in \mathbb{R}^N$, i.e., $\tau(v) = \alpha M(v) + (1 - \alpha)m(v)$, where for all $i \in N$

$$M_i(v) = v(N) - v(N \setminus \{i\}), \tag{8.4}$$

and

$$m_i(v) = max\{\ v(S) - \textstyle\sum_{j\in S\setminus\{i\}} M_j(v) \mid S \in 2^N, i \in S\}, \tag{8.5}$$

where $\alpha \in \mathbb{R}$ is such that $\sum_{i\in N} \tau_i(v) = v(N)$.

We show that the compromise value of a project game equals the project power measure of the corresponding project enabling task structure.

Theorem 8.4.1 *Let $\mathbb{T} \in PETS(N,p)$ and let $(N, v_{\mathbb{T}})$ be the corresponding project game. Then $\tau(v_{\mathbb{T}}) = \theta(\mathbb{T})$.*

Proof:
Note that

$$v_{\mathbb{T}}(N \setminus \{i\}) = \begin{cases} v_{\mathbb{T}}(N) - 1 & \text{if } i \in E(\mathbb{T}) \\ v_{\mathbb{T}}(N) & \text{otherwise} \end{cases} \tag{8.6}$$

Hence for $i \in N$

$$M_i(v_{\mathbb{T}}) = \begin{cases} 1 & \text{if } i \in E(\mathbb{T}) \\ 0 & \text{otherwise} \end{cases} \tag{8.7}$$

We will first show that

$$m_i(v_{\mathbb{T}}) = \begin{cases} 1 & \text{if } i \in CL(\mathbb{T}) \\ 0 & \text{otherwise} \end{cases} \tag{8.8}$$

Let $i \in N$ and let $S \in 2^N$ with $i \in S$. Obviously there are at least $v_{\mathbb{T}}(S)$ essential players in S and, hence $\sum_{j \in S \setminus \{i\}} M_j(v_{\mathbb{T}}) \geq v_{\mathbb{T}}(S) - 1$. We can conclude that $m_i(v_{\mathbb{T}}) \leq 1$ for all $i \in N$. Assume $i \in CL(\mathbb{T})$ and set $S^* = I(\mathbb{T}) \cup \{i\}$. Then by construction $|S^* \cap T_k| = |\{i\}| = 1$ for all $k \in C(\mathbb{T})$ and $|S^* \cap T_k| \geq 1$ for all $k \in P \setminus C(\mathbb{T})$. It follows that $v_{\mathbb{T}}(S^*) = 1$ and

$$\sum_{j \in S^* \setminus \{i\}} M_j(v_{\mathbb{T}}) = 0.$$

Hence $v_{\mathbb{T}}(S^*) - v_{\mathbb{T}}(S^* \setminus \{i\}) = 1$. We conclude that $m_i(v_{\mathbb{T}}) = 1$.

Assume that $i \notin CL(\mathbb{T})$. If $i \in I(\mathbb{T})$ then $\sum_{j \in S \setminus \{i\}} M_j(v_{\mathbb{T}}) = \sum_{j \in S} M_j(v_{\mathbb{T}}) \geq v_{\mathbb{T}}(S)$ and consequently $m_i(v_{\mathbb{T}}) \leq 0$. Finally assume that $i \in PL(\mathbb{T})$. Then there exists $k \in P$ such that $T_k \subset E(\mathbb{T})$ with $i \notin T_k$. For any $S \subset N$ with $i \in S$ we have,

$$v_{\mathbb{T}}(S) = min_{l \in \{1,\ldots,p\}} |T_l \cap S| \leq |T_k \cap S| = |T_k \cap (S \setminus \{i\})| \leq |E(\mathbb{T}) \cap (S \setminus \{i\})| = \sum_{j \in S \setminus \{i\}} M_j(v_{\mathbb{T}}),$$

Hence $m_i(v_{\mathbb{T}}) = 0$.

We are now ready to show that $\tau(v_{\mathbb{T}}) = \theta(\mathbb{T})$. Since $CL(\mathbb{T}) \subset E(\mathbb{T})$ it follows from (7.7) and (7.8) that for all $i \in CL(\mathbb{T})$ it holds that $M_i(v_{\mathbb{T}}) = m_i(v_{\mathbb{T}}) = 1$, for all $j \in I(\mathbb{T})$ it holds that $M_j(v_{\mathbb{T}}) = m_j(v_{\mathbb{T}}) = 0$, and for all $j \in PL(\mathbb{T})$ it holds that $M_j(v) = 1$ and $m_j(v) = 0$. Since the compromise value is efficient, we get

$$\sum_{i \in N} \tau_i(v_{\mathbb{T}}) = |CL(\mathbb{T})| + \alpha \cdot |PL(\mathbb{T})| = v_{\mathbb{T}}(N) = tot(\mathbb{T}).$$

Thus $\tau_i(v_{\mathbb{T}}) = \frac{tot(\mathbb{T}) - |CL(\mathbb{T})|}{|PL(\mathbb{T})|}$ for all $i \in PL(\mathbb{T})$. □

A game $v \in TU^N$ is called compromise admissible if

$$m(v) \leq M(v) \text{ and } \textstyle\sum_{\in N} m_i(v) \leq v(N) \leq \sum_{i \in N} M_i(v)$$

The class of compromise admissible games with player set N is denoted by CA^N. Let $\mathbb{T} \in PETS(N, p)$. Since $CL(\mathbb{T}) \subset E(\mathbb{T})$ it readily follows from (8.7) and (8.8) that $m(v_{\mathbb{T}}) \leq M(v_{\mathbb{T}})$. In addition it can easily be seen that

$$\sum_{i \in N} m_i(v_{\mathbb{T}}) = |CL(\mathbb{T})| \leq v_{\mathbb{T}}(N) \leq |E(\mathbb{T})| = \sum_{i \in N} M_i(v_{\mathbb{T}}).$$

Hence project games are compromise admissible.

8.4.2 Relation to the core

In this section we analyze the core of a project game and relate its structure to the project enabling task structure. First we show that project games are totally balanced.

The core $Core(v)$ [Gillies, 1953] of a game $(N, v_{\mathbb{T}})$ is the set of efficient allocations in which no coalition has an incentive to split off from the grand coalition N:

$$Core(v) = \{x \in \mathbb{R}^N | \sum_{i \in N} x_i = v(N), \sum_{i \in S} x_i \geq v(S) \text{ for all } S \in 2^N\}.$$

The core may be an empty set. If the core of a game is non-empty it is also referred to as a *balanced game*. For a game (N, v) and a coalition $T \subset N$ the subgame (T, v^T) is obtained by restricting v to subsets of T. A game (N, v) is *totally balanced* if for every $T \subset N$ its subgame (T, v^T) is balanced, i.e., if every subgame has a non-empty core.

We first illustrate concept of the core of a project game and its relation to critical task group vectors in Example 8.2.

Example 8.2:
Let $N = \{1, 2, 3, 4\}$. Consider $\mathbb{T} = (T_1, T_2, T_3, T_4) \in PETS(N, p)$ with $T_1 = \{1, 2\}, T_2 = \{1, 3\}, T_3 = \{1, 4\}$ and $T_4 = \{2, 3, 4\}\}$. Then $C(\mathbb{T}) = \{1, 2, 3\}$, $E(\mathbb{T}) = N$ and $CL(\mathbb{T}) = \emptyset$. We have

$$v_{\mathbb{T}}(S) = \begin{cases} 0 & \text{if} \quad |S| = 1 \\ 0 & \text{if} \quad |S| = 2 \text{ with } 1 \notin S \\ 1 & \text{if} \quad |S| = 2 \text{ and } 1 \in S \text{ or if } |S| = 3 \\ 2 & \text{if} \quad S = N \end{cases} \tag{8.9}$$

Let $x = (x_1, x_2, x_3, x_4) \in Core(v)$. Then $v(N) - x_1 = x_2 + x_3 + x_4 \geq v(\{2, 3, 4\}) = 1$, hence $x_1 \leq 1$. Since $v(S) = 1$ for all S with $|S| = 2$ containing player 1 it follows that $x_i \geq 1 - x_1$ for all $i \in \{2, 3, 4\}$. Thus $2 - x_1 = x_2 + x_3 + x_4 \geq 3 - 3x_1$, hence $x_1 \geq \frac{1}{2}$. It readily follows that

$$Core(v_{\mathbb{T}}) = conv(\{\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\}, \{1, 1, 0, 0\}, \{1, 0, 1, 0\}, \{1, 0, 0, 1\}\})$$

and

$$conv(\{e^{T_k} | k \in C(\mathbb{T})\}) = conv(\{\{1, 1, 0, 0\}, \{1, 0, 1, 0\}, \{1, 0, 0, 1\}\}),$$

hence $conv(\{e^{T_k} | T_k \in C(\mathbb{T})\}) \subsetneq Core(v_{\mathbb{T}})$. ◇

In general project games and all its subgames have a non-empty core as the following theorem shows.

Theorem 8.4.2 *Project games are totally balanced.*

Proof:
A project game $(N, v_{\mathbb{T}})$, with $\mathbb{T} = (T_1, ..., T_p)$, is the minimum of a finite set of additive games . Let $k \in \{1, ..., p\}$ and set $a_i = e_i^{T_k}$ for all $i \in N$. Define the additive game $w^k(S) = \sum_{i \in S} a_i$, then

$$v_{\mathbb{T}}(S) = min_{k \in \{1, ..., p\}} |T_k \cap S| = min\{w^k(S) | k \in \{1, ..., p\}\} \text{ for all } S \subset N. \tag{8.10}$$

Hence every project game is totally balanced [Kalai and Zemel, 1982]. □

In the next theorem we show that the convex hull of critical task group vectors of a project enabling task structure is a subset of the core of the corresponding project game.

Theorem 8.4.3 *Let $\mathbb{T} \in PETS(N, p)$. Then $conv(\{e^{T_k} | T_k \in C(\mathbb{T})\}) \subset Core(v_{\mathbb{T}})$.*

Proof:
Let $T_k \in C(\mathbb{T})$. It suffices to prove that $e^{T_k} \in Core(v_{\mathbb{T}})$. Clearly $\sum_{i \in N} e_i^{T_k} = |T_k| = v_{\mathbb{T}}(N)$. In addition it readily follows that

$$\sum_{i \in S} e_i^{T_k} = |S \cap T_k| \geq min_{l \in \{1,\ldots,p\}} |S \cap T_l| = v_{\mathbb{T}}(S) \quad \text{for all } S \subset N.$$

□

8.5 Remarks and observations

In this chapter we took another approach to determine the power or importance of players that are somehow 'connected' to a covert organization that conducts projects. We considered those facts that in reality can be (partially) known: the tasks making up the project and the individuals that enable them. We modeled such a situation as a project enabling task structure and analyzed the power of each player due to his structural position in this 'system'. Our project power measure provides an objective benchmark to determine which players to focus on given that a covert organization is conducting a project. For instance, if it is known that a certain country is in the process of building and manufacturing a nuclear bomb, it becomes imperative to find out which individuals enable which tasks (the tasks of such a project are generally widely known). Then it becomes possible to target those individuals and hinder the completion of the project.

Future research could incorporate other elements, i.e., it might be known that certain tasks in a project depend on other tasks, thus it could be useful to introduce this dependency into the model. Moreover the fact that there exists a social network among the players could also be taken into account, essentially combining the game theoretic network analysis approach we presented in chapter 7 and the project approach as presented in this chapter.

Bibliography

Z. Abuza. *Militant Islam in Southeast Asia.* London: Lynne Rienner Publishers, 2003.

R. Albert and A.L. Barabasi. Error and attack tolerance of complex networks. *Nature*, 406:378–382, 2000.

J.T. Allatta. *Structural analysis of communities of practice: an investigation of job title, location, and management intention. In Communities and Technologies, Huysman, M. Wenger, E., and Wulf, V. (Eds.).* Norwell, MA.: Kluwer Academic Publishers, 2003.

J.T. Allatta. *Worker Collaboration and Communities of Practice.* Ph.D. dissertation, Pennsylvania: University of Pennsylvania, 2005.

M.P. Allen. The identification of interlock groups in large corporate networks: Convergent validation using divergent techniques. *Social Networks*, 4:349–366, 1982.

R. Amer and J.M. Giminez. A connectivity game for graphs. *Mathematical Methods of Operation Research*, 60:453–470, 2004.

J. Arquilla and D. Ronfeldt. *Networks and Netwars.* Santa Monica, CA.: RAND monograph MR-1382, 2001.

V. Asal, B. Nussbaum, and D.W. Harrington. Terrorism as transnational advocacy: an organizational and tactical examination. *Studies in Conflict and Terrorism*, 30:15–39, 2007.

W.E. Baker and R. Faulkner. The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review*, 58:837–860, 1993.

T.T. Baldwin. The social fabric of a team-based m.b.a. program: Network effects on student satisfaction and performance. *The Academy of Management Journal*, 6:1369–1397, 1997.

F. Ball. Epidemics with two levels of mixing. *The Annals of Applied Probability*, 7:46–89, 1997.

H. Bar-Isaac and M. Baccara. How to organize crime. *Review of Economic Studies*, 75: 1039–1067, 2008.

A. Barnett. Safe at home? an experiment in domestic airline security. *Operations Research*, 49:181–195, 2001.

A. Bavelas. A mathematical model for group structure. *Human Organizations*, 7:16–30, 1948.

A. Bavelas. Communication patterns in task oriented groups. *Journal of the Acoustical Society of America*, 22:271–282, 1950.

J. Bearden and B. Mintz. *The structure of class cohesion: The corporate network and its dual. In Mizruchi, M.S. and Schwartz, M. (eds.), Intercorporate Relations: The Structural Analysis of Business.* Cambridge: Cambridge University Press, 1987.

M.A. Beauchamp. An improved index of centrality. *Behavioral Science*, 10:161–163, 1965.

A. Ben-David. Israel aims for 'new security reality' in gaza. *Jane's Defence Weekly*, 2009.

G. Bergantinos and E. Sanchez. How to distribute costs associated with a delayed project. *Annals of Operations Research*, 109:159–174, 2002a.

G. Bergantinos and E. Sanchez. Ntu pert games. *Operations Research Letters*, 30:130–140, 2002b.

P. Bergen. *The Osama Bin Laden I Know: and Oral History of al Qaeda's Leader.* New York: Free Press, 2006.

B. Bollobas. *Combinatorics: Set Systems, Hypergraphs, Families of Vectors and Probabilistic Combinatorics.* Cambridge: Cambridge University Press, 1986.

B. Bollobas. *Modern Graph Theory.* New York: Springer-Verlag, 1998.

P. Bonacich. *Using Boolean algebra to analyze overlapping memberships. In Schuessler, K.F. (Ed.).* San Francisco: Jossey-Bass, 1978.

P. Bonacich. Power and centrality: a family of measures. *American Journal of Sociology*, 92:1170–1182, 1987.

O. Bondareva. Some applications of linear programming methods to the theory of cooperative games. *Problemy Kibernet*, 10:119–139, 1963.

S.P. Borgatti. The key player problem. *In Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, R. Breiger, K. Carley, P. Pattison, (Eds.)*, 1: 241–252, 2003.

S.P. Borgatti and M.G. Everett. A graph-theoretic framework for classifying centrality measures. *Social Networks*, 28:466–484, 2006.

P. Borm, G. Owen, and S. Tijs. On the position value for communication situations. *SIAM Journal on Discrete Mathematics*, 5:305–320, 1992.

U. Brandes and T. Erlebach (Eds.). *Network Analysis: Methodological Foundations.* Berlin, Heidelberg: Springer-Verlag, 2005.

R. Branzei, V. Ferrari, and S. Tijs. Two approaches to the problem of sharing delay costs in joint projects. *Annals of Operations Research*, 109:359–374, 2002.

R.L. Breiger. *The Analysis of Social Networks. In Hardy, M. and Bryman, A. (Eds.). Handbook of Data Analysis.* London: Sage Publications, 2004.

G.G. Brown, W.M. Carlyle, R. Harney, E. Skroch, and R.K. Wood. Interdicting a nuclear weapons project. *Operations Research*, 57:866–877, 2009.

A.P.M. Cammaert. *Het Verborgen Front.* Leeuwarden: EISMA B.V., 1994.

K.M. Carley. Destabilization of covert networks. *Computational & Mathematical Organization Theory*, 12:51–66, 2006.

K.M. Carley, J. Reminga, and N. Kamneva. Destabilizing terrorist networks. *NAACSOS conference proceedings, Pittsburgh*, 2003.

F.R.K. Chung. Diameters of graphs: Old problems and new results. *Congressus Numerantium*, 60:295–317, 1987.

Y. Cohen and J. White. Hamas in combat. *Policy Focus*, 97, 2009.

A.H. Cordesman et al. *Lessons of the 2006 Israeli-Hezbollah War.* Washington D.C.: Center for Strategic and International Studies, 2007.

Council on Foreign Relations. Jemaah islamiyah. *Last retrieved May 2011 from http://www.cfr.org/indonesia*, 2009.

D.L. Craft et al. Analyzing bioterror response logistics: the case of anthrax. *Management Science*, 51:679–694, 2005.

M.L. von Creveld. *The Transformation of War.* New York: Free Press, 1991.

P. Cruickshank and M. Hage Ali. Abu musab al suri: Architect of the new al qaeda. *Studies in Conflict and Terrorism*, 30:1–14, 2007.

W. Enders and X. Su. Rational terrorists and optimal network structure. *Journal of conflict resolution*, 51:33–57, 2007.

D. Engelen. *De Nederlandse stay behind-organisatie in de koude oorlog.* 's Gravenhage: PIVOT-rapport nr. 166, 2005.

A. Estevez-Fernandez, P.E.M. Borm, and H.J.M. Hamers. Project games. *International Journal of Game Theory*, 36:149–176, 2007.

J.D. Farley. Breaking al qaeda cells: a mathematical analysis of counterterrorism operations. *Studies in Conflict and Terrorism*, 26:399–411, 2003.

T.L. Frantz and K.M. Carley. *A Formal Characterization of Cellular Networks.* Carnegie Mellon University, School of Computer Science (SCS), Institute for Software Research (ISR), Center for Computational Analysis of Social and Organizational Systems (CASOS) Technical Report CMU-ISRI-05109., 2005.

L.C. Freeman. A set of measures of centrality based on betweenness. *Sociometry*, 40: 35–41, 1977.

L.C. Freeman. *The Development of Social Network Analysis: A Study in the Sociology of Science.* Vancouver: Empirical Press, 2005.

G. Gambill. Sponsoring terrorism: Syria and hamas. *Middle East Intelligence Bulletin*, 4, 2002.

D.B. Gillies. *Some theorems on n-person games.* Ph.D. Thesis. Princeton, New Jersey: Princeton University Press, 1953.

A. Golan. *Operation Susannah.* New York: Harper & Row, Publishers, Inc., 1978.

D. Gomez et al. Centrality and power in social networks: a game theoretic approach. *Mathematical Social Sciences*, 46:27–54, 2003.

B. Grofman and G. Owen. A game theoretic approach to measuring centrality in social networks. *Social Networks*, 4:213–224, 1982.

H. Guetzkow and H.A. Simon. The impact of certain communication nets upon organization and performance in taks-oriented groups. *Management Science*, 1:233–250, 1955.

R. Gunaratna. *Inside Al Qaeda: Global Network of Terror.* Berkley Trade, 2003.

A.J. Hoffman and R.R. Singleton. Moore graphs with diameter 2 and 3. *IBM Journal of Research and Development*, 5:497–504, 1960.

S. Huisman and E.M. Smits. *Synthetische drugs en precursoren.* Driebergen: KLPD-Dienst Nationale Recherche., 2008.

International Crisis Group. Indonesia backgrounder: how the jemaah islamiyah terrorist network operates. *Asia report*, 43, 2002.

M.O. Jackson. *Social and Economic Networks.* Princeton, New Jersey: Princeton University Press, 2008.

B.R. Jasny and B. Ray. Life and the art of networks. *Science*, 301:1863, 2003.

L.K. (ed.) Johnson. *Strategic Intelligence: Covert action-beyond the veils of secret foreign policy.* Westport: Praeger Security International, 2007.

J. Jordan. When heads roll: Assessing the effectiveness of leadership decapitation. *Security Studies*, 18:719–755, 2009.

E. Kalai and E. Zemel. Totally balanced games and games of flow. *Mathematics of Operations Research*, 7:476–478, 1982.

T.H. Kean, L.H. Hamilton, and R. Ben-Veniste. *The 911 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States.* New York: W.W. Norton and Company, Inc., 2002.

D. Kinsella. The black market in small arms: Examining a social network. *Paper presented at the annual meeting of the International Studies Association*, 2005.

S. Koschade. Indonesia backgrounder: How the jemaah islamiyah terrorist network operates. *International Crisis Group*, 43, 2002.

S. Koschade. A social network analysis of jemaah islamiyah: the applications to counterterrorism and intelligence. *Studies in Conflict and Terrorism*, 29:559–575, 2006.

V.E. Krebs. Uncloaking terrorist networks. *First Monday*, 7:1–10, 2002.

R.H. Lester and A.A. Cannella. Interorganizational familiness: How family firms use interlocking directorates to build community-level social capital. *Entrepreneurship Theory and Practice*, 30:756–775, 2006.

J.H. Levine. The sphere of influence. *American Sociological Review*, 37:14–27, 1972.

M. Levitt. Hamas from cradle to grave. *The Middle East Quarterly*, 11:3–15, 2004.

K.Y. Lin, M. Kress, and R. Szechtman. Scheduling policies for an antiterrorist surveillance system. *Naval Research Logistics*, 56:113–126, 2009.

R. Lindelauf. Figthing irregulars: the critical role of network science. *Atlantisch Perspectief*, 2:19–23, 2009.

R. Lindelauf and I. Blankers. Key player identification: A note on weighted connectivity games and the shapley value. *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2010). IEEE*, pages 356–359, 2010.

R. Lindelauf, I. Blankers, P. Borm, and H. Hamers. On the optimal distribution of risk and information exchange in star networks. in v.s. subramanian and a. kruglanski (eds.). *Proceedings of the 2nd International Conference on Computational Cultural Dynamics (ICCCD). IEEE*, pages 45–48, 2008.

R. Lindelauf, P. Borm, and H. Hamers. The influence of secrecy on the communication structure of covert networks. *Social Networks*, 31:126–137, 2009a.

R. Lindelauf, P. Borm, and H. Hamers. *On Heterogeneous Covert Networks. In: N. Menon, J.D. Farley, D.L. Hicks, & T. Rosenorn (Eds.), Mathematical Methods in Counterterorrism.* Vienna: Springer-Verlag, 2009b.

R. Lindelauf, P. Borm, and H. Hamers. One-mode projection analysis and design of covert affiliation networks. *CentER Discussion Paper*, 53:1–23, 2010.

R. Lindelauf, P. Borm, and H. Hamers. *Understanding terrorist network topologies and their resilience against disruption. In: Counterterrorism and Open Source Intelligence Memon, N.; Wiil, U.(Eds.).* Springer, to appear, 2011.

J. Magouirk, S. Atran, and M. Sageman. Connecting terrorist networks. *Studies in Conflict and Terrorism*, 31:1–16, 2008.

M. Mariotti. Nash bargaining theory when the number of alternatives can be finite. *Social Choice and Welfare*, 15:413–421, 1998.

G. Martin. *Understanding terrorism: challenges, perspectives, and issues.* Los Angeles: Sage Publications, 2006.

B. McAllister. Al qaeda and the innovative firm: Demythologizing the network. *Studies in Conflict and Terrorism*, 27:297–319, 2004.

G.H. McCormick and G. Owen. Security and coordination in a clandestine organization. *Mathematical and computer modeling*, 31:175–192, 2000.

M. Miller and J. Siran. Moore graphs and beyond: A survey of the degree/diameter problem. *The Electronic Journal of Combinatorics*, 14:1–61, 2005.

Miller, G. and Meyer, J. Document links al qaeda paymaster, 9/11-plotter. *Last retrieved May 2011 from http://articles.latimes.com/2002/sep/27/nation/na-intel27*, 2002.

B. Mintz and M. Schwartz. Interlocking directorates and interest group formation. *American Sociological Review*, 46:851–868, 1981.

S. Mishal and M. Rosenthal. Al qaeda as a dune organization: Toward a typology of islamic terrorist organizations. *Studies in Conflict and Terrorism*, 28:275–293, 2005.

M.S. Mizruchi. Review of dan clawson, alan neustadtl, and denise scott, money talks: Corporate pacs and political influence. *Administrative Science Quarterly*, 39:176–179, 1994.

M.S. Mizruchi and D. Bunting. Influence in corporate networks: An examination of four measures. *Administrative Science Quarterly*, 26:475–489, 1981.

M.S. Mizruchi and D. Bunting. Who controls whom?: An examination of the relation between management and boards of directors in large american corporations. *Academy of Management Review*, 8:426–435, 1983.

C. Morselli, C. Giguere, and K. Petit. The efficiency/security trade-off in criminal networks. *Social Networks*, 29:143–153, 2007.

R.B. Myerson. Graphs and cooperation in games. *Mathematics of Operation Research*, 2:225–229, 1977.

R.B. Myerson. Conference structures and fair allocation rules. *International Journal of Game Theory*, 9:169–182, 1980.

M.W. Nance. *Terrorism recognition handbook: a practitioner's manual for predicting and identifying terrorist activities.* Taylor & Francis Group, Boca Raton., 2008.

M. Natarajan. Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. *Journal of Quantitative Criminology.*, 22: 171–192, 2006.

J. von Neumann and O. Morgenstern. *Theory of games and Economic Behaviour.* Princeton, New Jersey: Princeton University Press, 1944.

M.E.J. Newman. Analysis of weighted networks. *Physical Review E*, 70:056–131, 2004.

M.E.J. Newman, A.L. Barabasi, and D.J. Watts. *The Structure and Dynamics of Networks.* Princeton, New Jersey: Princeton University Press, 2006.

G. Owen. Values of graph-restricted games. *SIAM Journal on Algebraic and Discrete Methods*, 7:210–220, 1986.

G. Owen. *Game Theory.* San Diego: Academic Press, 2001.

D.H. Petraeus et al. *The U.S. Army Marine Corps Counterinsurgency Field Manual.* Chicago: University of Chicago Press, 2007.

J. Raab and H. Brinton Milward. Dark networks as problems. *Journal of Public Administration*, 13:413–439, 2001.

B.K. Reed. *Models for proliferation interdiction response analysis.* Monterey, CA.: Naval Postgraduate School, 2004.

J. Rollins. Al qaeda and affiliates: historical perspective, global presence, and implications for u.s. policy. *Congressional Research Service (CRS) Reports and Issue Briefs*, 2010.

M. Sageman. *Understanding terror networks.* Philadelphia: University of Pennsylvania Press, 2004.

M. Sageman. *Leaderless Jihad: Terror Networks in the Twentyfirst Century.* Philadelphia: University of Pennsylvania Press, 2008.

A.P. Schmid and A.J. Jongman. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature.* New Jersey: Transaction Books, 1988.

J. Scott. *Social Network Analysis: A Handbook. 2nd Ed.* Newberry Park, CA: Sage, 2000.

E. Seville, D. Brunsden, A. Dantas, and J. Le Masuer. *Building Organisational Resilience: a Summary of Key Research Findings.* Research Report, 2006.

L. Shapley. A value for n-person games. *Annals of Mathematics Studies*, 28:307, 1953.

L. Shapley. On balanced sets and cores. *Naval Research Logistics Quarterly*, 14:453, 1967.

P. Siarry. *Multiobjective Optimization. Principles and Case Studies.* Berlin Heidelberg: Springer-Verlag, 2003.

M. Sparrow. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, 13:251–274, 1991.

K. Stephenson and M. Zelen. Rethinking centrality: methods and examples. *Social Networks*, 11:1–37, 1989.

S.H. Strogatz. Exploring complex networks. *Nature*, 410:268–276, 2001.

S. Swanson. Viral targeting of the ied social network system. *Small Wars Journal*, 8: 2–17, 2007.

H.C. Tijms. *A first course in Stochastic Models.* West Sussex: John Wiley & Sons, 2003.

S.H. Tijs. *Bounds for the core and the $\tau-$value. In O. Moeschlin and D. Pallaschke (Eds.), Game Theory and Mathematical Economics.* North-Holland, Amsterdam, 1981.

M. Tsvetovat and K.M. Carley. Structural knowledge and success of anti-terrorist activity: The downside of structural equivalence. *Journal of Social Structure*, 6:2, 2005.

D. Tucker. What is new about the new terrorism and how dangerous is it? *Terrorism and Political Violence*, 13:1–14, 2001.

L. Vidino. Current trends in jihadi networks in europe. *Terrorism Monitor*, 20:8–11, 2007.

S. Wasserman and K. Faust. *Social Network Analysis, methods and applications.* Cambridge: Cambridge University Press, 1994.

D.J. Watts. Collective dynamics of 'small-world' networks. *Nature*, 393:440–442, 1998.

D.J. Watts. The 'new' science of networks. *Annual Review of Sociology*, 30:243–270, 2004.

T. Weiner. *Legacy of ashes: the history of the CIA.* New York: Random House, Inc., 2007.

B. Wellman and S.D. Berkowitz. *Social Structures: A Network Approach.* Cambridge: Cambridge University Press, 1988.

W.M. Wise. Indonesia's war on terror. *United States-Indonesia Society*, 2005.

G.L. Zacharias et al. *Behavioral Modeling and Simulation: From Individuals to Societies.* National Academy of Sciences, 2008.

S. Zuhur. *Hamas and Israel: conflicting strategies of group-based politics.* Strategic Studies Institute: U.S. Army War College, 2008.

O. Zwikael. Al qaeda's operations: Project management analysis. *Studies in Conflict and Terrorism*, 30:267–280, 2007.

Author index

Myerson, R.B., 105

Nance, M.W., 68
Natarajan, M., 92
Newman, M., 8, 91
Nussbaum, B., 18

Owen, G., 19, 91

Petraeus, D.H., 4

Raab, J., 19
Ray, B., 91
Ronfeldt, D., 6, 20, 68

Sageman, M., 18, 19
Schmid, 3
Siarry, P., 26
Simon, H.A., 20
Singleton, R.R., 34
Siran, J., 20, 33
Sparrow, M., 19, 91
Strogatz, S.H., 91
Su, X., 19
Szechtman, R., 67

Tijms, H.C., 31
Tijs, S., 139
Tsvetovat, M., 18
Tucker, D., 18, 67

Vidino, L., 6

Wasserman, S., 101
Weiner, T., 17

Zacharias, G.L., 91

Subject index